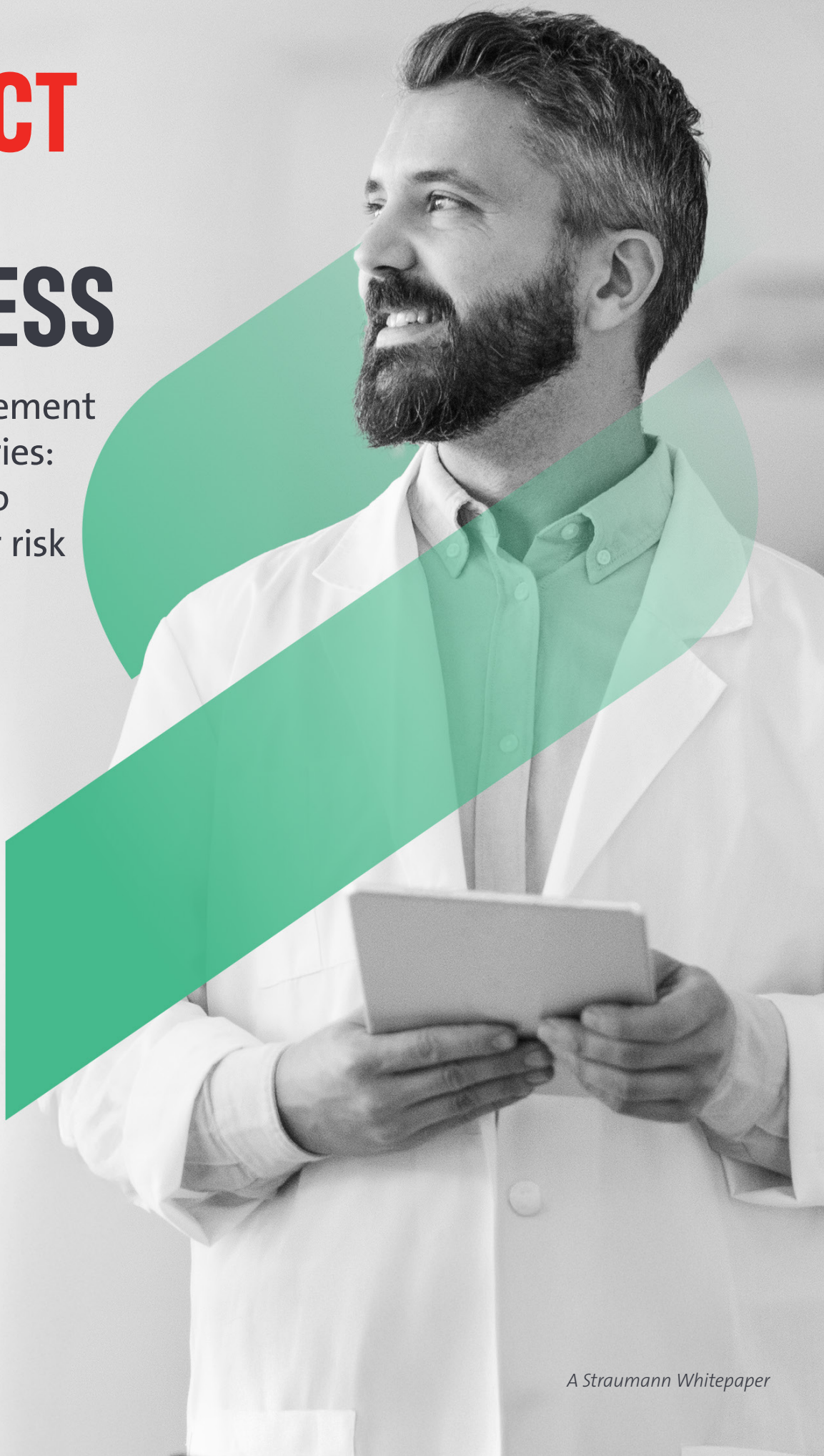
straumann

PROTECT YOUR BUSINESS

Practice Management White Paper Series: A DSO's guide to managing cyber risk



CARESTACK

A Straumann Whitepaper

A TRUSTED STRAUMANN PARTNER.

Straumann has partnered with CareStack to revolutionize the standard of managing a dental organization.

CareStack is an award-winning cloud-based practice management software (PMS) trusted by 1,500+ dental practices and organizations (DSOs) to streamline their operations.

To discover more, please visit our CareStack webpage:
www.straumann.com/en/discover/carestack.html

CONTENTS

1. OVERVIEW: HOW TO PROTECT YOUR BUSINESS

When it comes to cybersecurity, DSOs must understand that being the target of a cyberattack is a matter of "when" not "if". To protect themselves from the growing and ever-evolving cyber threat, DSOs should adopt several principles:

UNDERSTAND THE CYBER RISK

Stay up to date with the threats in your sector. Understanding the potential risks helps you better prepare.

SAFER IN THE CLOUD

Combine trusted cloud solutions hosted on resilient, secure cloud infrastructures with a "zero trust" approach to cybersecurity for the best cybersecurity posture.

CHOOSE AN APPLICATION THAT IS SECURE BY DESIGN

CareStack prioritizes cybersecurity at every stage of the software lifecycle—from design and development, through access control, monitoring and incident response.

PROTECT YOUR DATA

Good information governance policies, comprehensive encryption and adherence with industry certifications and regulatory frameworks underpin best practice.

ENACT STRINGENT USER MANAGEMENT AND ACCESS CONTROL

Advanced IAM solutions, multi-factor authentication, role-based access controls, endpoint security and continuous monitoring help to protect against unauthorized access.

AN INTEGRATED SOLUTION HELPS TO MINIMIZE COMPLEXITY

As an all-in-one practice management system, CareStack enables DSOs to reduce complexity and overheads, simplify system management and take a more integrated approach.

EXCELLENT, RESPONSIVE SUPPORT IS A MUST

By choosing CareStack and Straumann, DSOs are assured of high-quality, highly responsive onboarding and ongoing application management and continued support with access to the best cybersecurity and application expertise.

*This white paper complements the Cybersecurity CareStack Straumann technical white paper, validating technical PMS aspects, such as data protection, policies and standards, proactive and reactive security, software supply chain, customer facing application security, compliance, and local privacy rules.

2. UNDERSTANDING CYBER RISK

Cyberattacks can result in financial losses, business disruption, data theft and reputational damage. With rising numbers of attacks and ever-evolving threats, the need to protect your dental organization from cyberattack has never been more acute.

Recent high-profile cyberattacks and data breaches in our sector have highlighted the increased risk of malicious cyber activity for dental practices and dental services organizations (DSOs).

In April 2023, the DSO Aspen Dental was subject to a cyberattack which shut down its appointment scheduling systems, phone systems and other business applications.[1] With the group's practices numbering over 1,000 across 45 states, the subsequent disruption and the threat of data loss was significant.

In September 2023, the dental and medical supply business Henry Schein suffered a data breach in which personal data of nearly 30,000 employees and their families was stolen[2]. The theft included credit and debit card numbers, the associated security codes, passwords and PINs and shut down the company's e-commerce platforms. The disruption led the business to lower its sales expectations for FY 2023 by $350 million to $400 million for Q4, with shares down 7.3 percent.[3]

2.1. THE COST OF A CYBERBREACH

DSOs are not alone in this. Malicious cyber activity has spiked in recent years. Forbes magazine reports from 2021 to 2023, there was a 72% increase in data breaches globally[4]. The cost of incidents has also shot up. In April 2024, the IMF's Global Financial Stability Report made it clear that the risk of extreme losses from cyber incidents has more than quadrupled since 2017 to $2.5 billion. Small and mid-size businesses can face similarly grievous costs. IBM's 2023 Cost of a Data Breach Report estimates the average impact of a data breach on organizations with fewer than 500 employees at $3.31 million.[5]

Affected organizations must find reactive emergency expenditure to hire cyber experts who can investigate issues, restore systems and recover data. Added to this, the cost of fines resulting from non-compliance with data governance and industry standards can be significant. For example, in the healthcare sector, **the average HIPAA violation fine following a data breach was $98,643** in 2022, according to a Corlette report. Most of these HIPAA violation fines were levied on small businesses. Indirect losses, including reputational damage or security upgrades, push the cost of a cyber breach significantly higher.

CareStack gives us a sense of security with public health information. Before, being on different servers, you had to share that information via email and we all know that emails are not as secure as they could be.

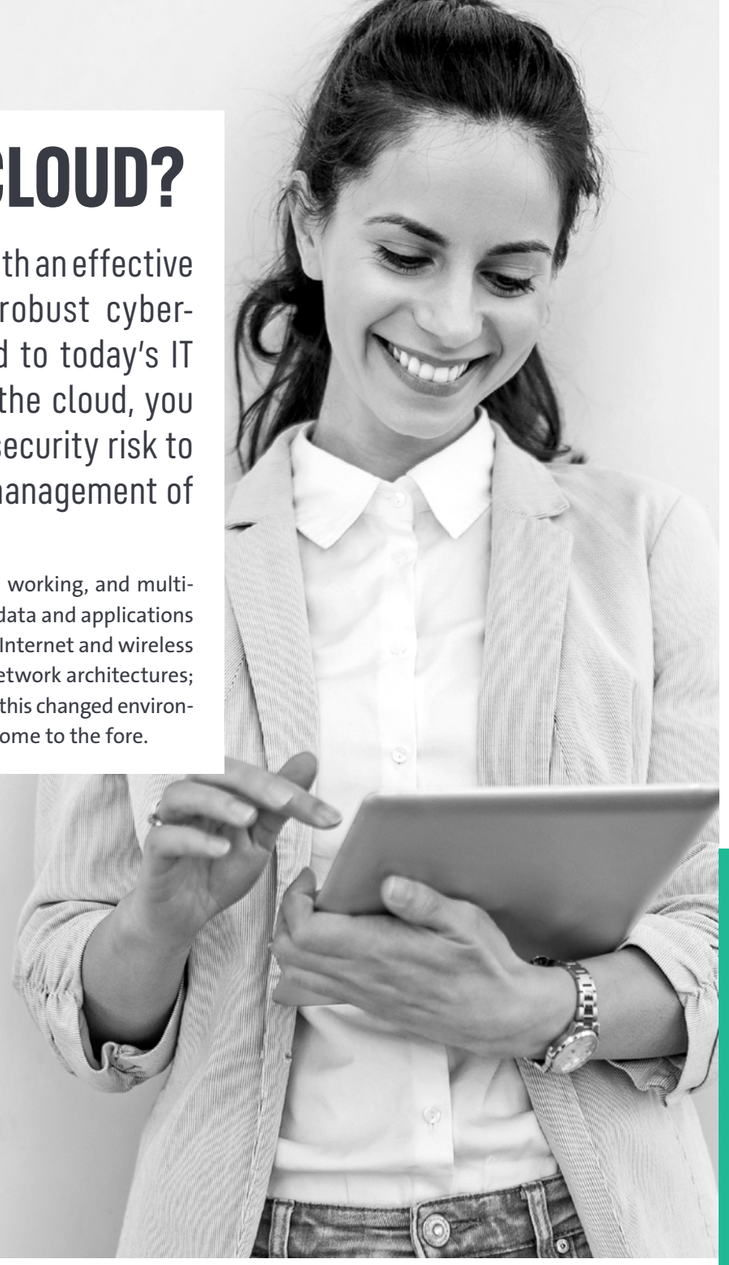
Dental Depot Group Practice, a multi-speciality US dental practice chain, based in Oklahoma City, with 30+ locations (with 5 locations using CareStack)

*This white paper complements the Cybersecurity CareStack Straumann technical white paper, validating technical PMS aspects, such as data protection, policies and standards, proactive and reactive security, software supply chain, customer facing application security, compliance, and local privacy rules.

3. SAFER IN THE CLOUD?

Trusted cloud solutions combined with an effective "zero trust" approach deliver a robust cyber-security stance that is well suited to today's IT environments. Plus, by moving to the cloud, you transfer a good deal of your cybersecurity risk to your cloud provider – putting the management of it into the hands of experts.

The way we work has changed: remote and hybrid working, and multi-site collaboration is the norm. Users need to access data and applications even when outside traditional network perimeters. Internet and wireless connectivity and mobile endpoints have changed network architectures; perimeters have become fuzzier and more porous. In this changed environment, new cybersecurity challenges and solutions come to the fore.



THE SECURITY ADVANTAGES OF CLOUD SOLUTIONS

As well as being more agile and scalable, cloud computing offers significant cybersecurity benefits. The major public clouds, including Microsoft Azure, are hosted in state-of-the-art datacenters with multiple levels of failover and redundancy built in. This type of resilience would be prohibitively expensive – if not impossible – to replicate in an on-premises environment.

These **cloud infrastructures offer options for compute, storage, backups and redundancy which are highly configurable**, so you can maintain data sovereignty and data residency in such a way that it meets the data laws or regulatory requirements which apply to your business. Integrated security tools available with the cloud platform offer **enterprise-grade security in an affordable and accessible way**.

In addition, by switching to a cloud solution, you eliminate many of the problems associated with on-premises solutions. Because data is no longer stored onsite in on-premises severs or PCs, the risks associated with physical theft, damage or tampering are reduced (assuming your devices and cloud applications are protected by appropriate user and access management and multi-factor authentication).

Using a cloud-hosted application means that your team can access it anywhere, anytime (with the right permissions). Staff are no longer tempted to share information by insecure methods, such as by email, because they can access what they need when they need it wherever they are.

Another significant benefit of cloud solutions is automatic updates. Instead of relying on your staff to apply security patches in good time, switching to a cloud-based solution ensures this is all done centrally and automatically for you. As a result, **known vulnerabilities which might be exploited by hackers are closed faster**.

Effective backups are your last line of defense in your cybersecurity strategy – offering a possibility to restore your systems, applications and data if the worst should happen. The US National Institute of Standards and Technology (NIST) says that, in cases of ransomware attack, hardware failure, and accidental or intentional data destruction, tested backups are vital for ensuring that organizations can quickly recover operational functionality after a cybersecurity incident[6]. Here, again, cloud solutions offer an advantage, with many offerings built-in, automated options for backup and recovery.

HOW CARESTACK HELPS YOU TO PROTECT YOUR BUSINESS

As a cloud solution, the all-in-one practice management software CareStack offers all these advantages and more. CareStack is hosted in Microsoft Azure infrastructure, leveraging its robust security features and compliance certifications (including ISO 27001, SOC 1/2/3, and HIPAA). This ensures that CareStack meets industry-leading standards for security, data management and reliability.

CareStack leverages the Microsoft Azure Healthcare platform to replicate all user data. Designed specifically for the healthcare industry, this platform provides a secure and compliant environment for storing and managing sensitive data. Your data is always backed up and protected and is accessible only by authorized users. This is especially important when handling patient health information which is specifically protected by law.

CareStack's always-on backups free staff from the time-consuming and fallible process of manual backups that used to be the norm. By eliminating the potential for human error, backup and restore capabilities are much more robust. Ensuring that you have an effective backup solution like this helps to mitigate the risk of ransomware viruses, which have become a major threat to small businesses around the globe.

* This white paper complements the Cybersecurity CareStack Straumann technical white paper, validating technical PMS aspects, such as data protection, policies and standards, proactive and reactive security, software supply chain, customer facing application security, compliance, and local privacy rules.

3.1 CHOOSE AN APPLICATION THAT IS SECURE BY DESIGN

Choosing the right business application and keeping it up to date with the latest security patches is critical to establishing a good cybersecurity posture. That's why IT leaders are increasingly prioritizing cybersecurity, when making purchasing decisions. Look for "secure by design" development principles, strong data protection capabilities, automatic security updates and a strong security culture.

Network and application cyberattacks are common in the healthcare sector. Statista data from 2022 shows that they accounted for the vast majority of attacks (63 percent)[7]. These risks were confirmed by 2024 Omdia research published in the Financial Times which reported the two most common type of cyberbreaches in healthcare are hacking and supply chain attacks[8]. With these risks predominating, the need to choose the right practice management software is critical to a DSO's cybersecurity posture.

The supply chain risk: Are you the weakest link?
It can be tempting to think that, as a small business, you are not worth the attention of cyber attackers. However, it simply isn't the case. Cyberattackers will target entire supply chains through their "weakest link". Even if a business isn't the attackers' ultimate target, it can still find itself compromised as a steppingstone to a larger target.

Worse, this way of thinking often leads small and mid-size businesses to deprioritize cybersecurity. Expert Insights explains, "**Smaller healthcare organizations are being hit hardest by cyberattacks.** Smaller organizations tend to have smaller budgets for cybersecurity, making them a prime target for malicious actors.[9]"

How to respond: Choose the right PMS
CareStack incorporates security best practices into every stage of its software development lifecycle, ensuring that products are secure by design. It follows secure development practices, including conducting regular security audits, performing code reviews, and employing secure coding standards. This proactive approach helps prevent security issues from arising during development and deployment. To strengthen this approach, CareStack conducts regular security awareness training for all employees to educate them on the latest security threats and best practices. This helps create a security-conscious culture and reduces the risk of human error leading to security incidents.

The application is cloud-hosted, making use of enterprise-grade security tooling and ensuring compliance with international cybersecurity and data protection standards. CareStack's cloud infrastructure employs security measures including user-specific access controls to protect the servers and network infrastructure where patient data is stored.

Data is further protected through encryption in transit and at rest. This encryption ensures that sensitive information remains secure and unreadable to unauthorized parties. Dynamic authentication schemes ensure that data continues to be protected even in the case of network intrusion. The authentication schemes between the CareStack practice management software and its API are dynamically generated and timestamped to prevent replay attacks (when a cyberattacker intercepts a network communication). Encryption keys are regularly rotated to prevent compromise over time, ensuring the continued security of data exchanges.

In this way, CareStack offers protection against the most common types of cyberattack affecting healthcare organizations, including DSOs. By opting for CareStack as your all-in-one practice management system, you have a great starting point when it comes to strengthening your overall cybersecurity posture.

* This white paper complements the Cybersecurity CareStack Straumann technical white paper, validating technical PMS aspects, such as data protection, policies and standards, proactive and reactive security, software supply chain, customer facing application security, compliance, and local privacy rules.

3.2 PROTECT YOUR DATA

Data governance is critical for DSOs, which typically hold a great deal of personal and sensitive information about patients and staff, as well as financial data. Efforts must be made to protect patient data, privacy and confidentiality. Only in this way can DSOs hope to avoid the heavy fines and reputational damage associated with a cyberbreach.

According to the HIPAA Journal, the industry's high volume of monetizable data is a big draw for cyber-attackers.[10] Dental practices and DSOs typically hold a great deal of valuable and personal patient information, including names, addresses, contact details, social security numbers, payment information, credit card and debit card details, health records, passwords and PINs. This large quantity of high-value information makes DSOs a target for both state-sponsored actors and cybercriminals.

Given the potential distress to patients and the financial penalties associated with a data breach, DSOs of all sizes must put measures in place to protect the data they hold. This includes strict controls to protect data from exfiltration as well as post-attack remedial solutions for backup and restore.

Never pay a ransom: get your backup and restore right instead
The healthcare sector has been made an even more attractive target to cyberattackers because of its historical response to ransomware attacks.

Ransomware is a specific type of malware used by hackers to encrypt data until the victim pays a ransom to unlock it. Healthcare boasts a higher-than-average probability that extortion demands will be met to prevent the release of locked or stolen data.

DSOs should heed NIST advice that businesses should never pay ransomware demands.[11] Any payment to cybercriminals is likely to be used to finance further criminal activity – making the cybersecurity environment more dangerous for everyone.

If that wasn't reason enough not to pay ransomware demands, the fact a payment is unlikely to unlock or restore data should be decisive. Proofpoint research shows that even after paying a ransom, data is often not unlocked. Of the 58 percent of organizations globally that tried to negotiate with their attackers in 2022, only 54 percent regained access to their data and systems after the first payment.[12]

Instead, DSOs should work with their solution providers to get the right backup and restore processes in place. This is a much better – and more reliable – last line of defense than making payments to cybercriminals.

How CareStack helps you to protect your data
CareStack helps DSOs to get the first lines of defense right, too. With CareStack you can protect the data you hold through a variety of approaches, effectively offering a "defense in depth" solution.

Encryption of data is a cornerstone of CareStack's approach. The solution uses strong encryption mechanisms when data is both in transit and at rest. Data is encrypted using industry-standard algorithms (e.g., AES-256) to ensure that it remains secure and unintelligible to unauthorized parties.

Access to data is another cornerstone of good information governance. CareStack's function-ality around identity and access management, endpoint security and user activity monitoring is particularly strong.

The company's commitment to good information governance is evident in CareStack's adherence to industry certifications including ISO 27001, HIPAA, GDPR, CCPA and SOC 2 Type I. These certifications validate its stringent security controls and best practices – so you know that all your data held in your CareStack practice management system is protected to the highest standards.

Furthermore, CareStack conducts regular audits and compliance checks on a quarterly basis. This ongoing commitment to compliance helps maintain compliance with regulation and trust in its security measures.

We wanted a shared system across locations, data analysis within one platform, reduced bolt-on services – so many things that CareStack delivers. We now have visibility that we didn't have before.

Dental Depot Group Practice, a multi-speciality US dental practice chain, based in Oklahoma City, with 30+ locations (with 5 locations using CareStack)

*This white paper complements the Cybersecurity CareStack Straumann technical white paper, validating technical PMS aspects, such as data protection, policies and standards, proactive and reactive security, software supply chain, customer facing application security, compliance, and local privacy rules.

3.3 ENACT STRINGENT USER MANAGEMENT AND ACCESS CONTROL

Ensuring access to systems and data is permitted only for authorized users is an essential part of cybersecurity best practice. DSOs need to have a comprehensive overview of users and devices on their network, as well as putting in place policies and procedures to limit access to systems and data in a way that empowers users while minimizing risk.

Understanding the phishing risk
Phishing attacks can use a variety of communication mechanisms – including email, SMS and social media – to target individuals. Cybercriminals often pose as legitimate organizations to trick victims into disclosing password and payment details or to download malware by clicking on a link or downloading a file containing malware.

More sophisticated phishing attacks in which cybercriminals research their victims and tailor phishing communications accordingly are increasingly common. "Big game phishing" attempts to reel in senior, IT or financial targets in your organization through personalized approaches, while phishing based on "social engineering" uses information available on social media accounts to make approaches to victims more targeted and convincing.

By investing in staff awareness training, you can help your staff to learn to spot suspicious emails, communications, websites and links.

At the same time, you also need to put measures in place to support and protect your staff.

Adopting a policy of "least privilege" is a good starting point. A least privilege approach minimizes the systems and data to which individual users have access so that if a user account is compromised, the damage is limited. This should be paired with an active user onboarding, review and offboarding policies and procedures as well as regular network scans to detect devices on the network so that you can proactively remove users, devices and permissions that are no longer required.

Other measures include email filtering; anti-malware and anti-virus software on all devices; multi-factor authentication; ensuring your single sign-on access policies are adequate; allowing users to only install trusted applications; ensuring all staff know how to respond to an incident; and encouraging an incident reporting culture.

By choosing a practice management system that supports these measures, you can help to strengthen your organization's cybersecurity posture.

We've reduced bolt-on services that were causing additional payroll dollars, all of those are vendor relationships we no longer have to manage.

Dental Depot Group Practice, a multi-speciality US dental practice chain, based in Oklahoma City, with 30+ locations (with 5 locations using CareStack)

How CareStack helps you to better manage and control users and access
CareStack is inherently more secure since it offers an all-in-one solution; meaning fewer access policies to manage and user identities to administer. Less complexity means less opportunity for error or vulnerabilities.

CareStack utilizes advanced identity and access management (IAM) solutions to manage user identities and control access to critical systems and data. This includes implementing policies for strong password management, regular access reviews, and automated provisioning and deprovisioning of user accounts.

In addition, CareStack employs multi-factor authentication and role-based access controls to ensure that only authorized personnel have access to sensitive information. As part of onboarding, CareStack implements comprehensive endpoint security measures, including antivirus and anti-malware solutions, to protect all devices connected to your network. This ensures that all endpoints are secure and monitored for potential threats.

Continuous monitoring of user activity enables us to detect any suspicious behavior and prevent unauthorized access or data breaches. By keeping a close eye on user actions, we can quickly identify and respond to potential security threats.

This layered approach to security helps to prevent unauthorized access and protects critical data.

*This white paper complements the Cybersecurity CareStack Straumann technical white paper, validating technical PMS aspects, such as data protection, policies and standards, proactive and reactive security, software supply chain, customer facing application security, compliance, and local privacy rules.

3.4 AN INTEGRATED SOLUTION HELPS TO MINIMIZE COMPLEXITY

One of the most compelling reasons for switching to CareStack is the full spectrum of dental practice management features it offers – benefiting dentists and care support staff, operational staff, senior managers and patients alike. This delivers numerous advantages, including around cybersecurity.

Simplifying a practice's IT estate with a unified practice management system like CareStack doesn't only bring efficiency, productivity and customer experience benefits. It also helps to simplify cybersecurity and reduce risk.

An all-in-one solution

CareStack is a comprehensive practice management system, spanning all aspects of a dental business – including marketing, onboarding, bookings, scheduling, payments, plans, claims and reporting. As a result, CareStack often replaces multiple applications with a single, integrated practice management solution.

As well as making life easier for users, who need only learn one piece of software, and making comprehensive reporting easier, a single all-in-one solution enables practices to simplify their IT estate.

Adopting CareStack's cloud-based practice management solution enables organizations to sunset legacy practice management systems and other third-party solutions.

This is important because each application comes with its own risks and vulnerabilities and its own update and patching requirements. Furthermore, any integrations between those applications will have their own risks, vulnerabilities and patching requirements. The fewer vendors you need to manage and the fewer applications you need to keep up to date, the easier it is to stay ahead of cyberattackers. With CareStack you have only one supplier and one software to manage.

Furthermore, when you implement CareStack, you can integrate systems and data across multiple locations. Instead of data being held locally on servers and desktop PCs, data is held securely in the cloud and only accessed by authorized users when needed. This eliminates the data risk associated with holding databases on physical machines on premises. It also eliminates clumsy workarounds that staff might develop to share data.

At the same time, the financial gains are considerable with CareStack on DSOs consolidating their systems. A Total Economic Impact™ study conducted by Forrester Consulting on behalf of Straumann in October 2023 found that a typical organization can save $282,400 on licensing and maintenance costs on a risk-adjusted basis.[13] These results are based on a composite organization representative of interviewed customers, assumed to have 10 locations, over three years.

3.5 EXCELLENT, RESPONSIVE SUPPORT IS A MUST

Software applications require ongoing maintenance and development if they are to stay ahead of cybersecurity threats and close vulnerabilities as they become known. Cloud solutions offer an advantage here since updates and security patches to close known vulnerabilities can be applied automatically. However, to take advantage of this, DSOs must choose a supplier that is committed to maintaining the highest standards of application management.

The challenge of application management

For software vendors and their customers, it is a constant race to close down vulnerabilities and protect against new forms of attack. With on-premises software, the onus falls on local IT teams to keep your application up to date and known vulnerabilities are patched as soon as possible, so they can't be exploited by hackers.

However, **cloud solutions make it easier for DSOs to stay ahead of cyberattackers**. With cloud-based software like CareStack, the platform and application are updated centrally by the provider. This means your teams no longer must worry or stay on top of the latest security updates. Instead, they are freed to concentrate on more strategic and proactive value-adding work.

*This white paper complements the Cybersecurity CareStack Straumann technical white paper, validating technical PMS aspects, such as data protection, policies and standards, proactive and reactive security, software supply chain, customer facing application security, compliance, and local privacy rules.

CASE STUDY: WORKING WITH A VENDOR THAT RESPONDS TO SECURITY THREATS QUICKLY

CareStack integrates with clearing houses to automatically process claims relating to dental treatment payments. When Change Healthcare (CHC), one of the country's largest clearing houses, was hit by a cyberattack on February 21, 2024, it had to isolate its systems.[14] As a result, practice management and other systems that utilize CHC's services were blocked, bringing vital revenue cycle processes to a halt.

Understanding the severe impact this would have on our customers' livelihood and patient care, CareStack acted quickly. The in-app notification system sent messages about CHC's outage to every customer in real-time to notify them about the situation. A form offering the option to reroute claims temporarily through another clearing house was created. Utilizing our cloud platform, changes could be quickly and easily implemented for any customer wishing to make the move. Throughout, CareStack support teams were available to answer questions and educate users on the new processes.

Change Healthcare allegedly paid a $22 million ransom[15] but, thanks to the quick action and dedication of the CareStack team, our customers were not held to ransom as well.

reduces the risk of exploitation. Furthermore, CareStack's vulnerability management programs are regularly updated to identify and address potential security weaknesses. By staying ahead of emerging threats, CareStack proactively protects your systems from vulnerabilities.

That's an important cost avoidance for DSOs because IT and cybersecurity expertise doesn't come cheap. Forbes estimates that the median salary for cybersecurity analysts in 2022 was $112,000 p.a. Multiply this salary by the number of people required to provide the necessary levels of 24/7/365 service and you can see why appropriate cybersecurity expertise is beyond the realms of most practices' budgets.

Cybersecurity experts are also in high demand. The growing skills gap makes it increasingly difficult to recruit and retain the right talent, even in sectors perceived to be attractive to tech talent (of which the dental sector is not one).

Furthermore, by moving to a cloud solution, practices offload the responsibility for purchasing, maintaining and protecting on-premises servers, associated hardware and systems. Because you have eliminated the need for on-premises servers and other associated infrastructure, your teams don't need to worry about security updates to those devices, hardware or operating systems – that's all the responsibility of your cloud provider.

This helps DSOs to reduce the potential for human error while accessing best-in-class, enterprise-quality security. Plus, it frees even more time for your inhouse IT team to concentrate on strategic and proactive value-adding work.

Backed up with excellent support

As well as offloading a lot of the day-to-day application and infrastructure management, when you choose CareStack as your practice management solution, you gain the added benefit of excellent support.

CareStack support extends from onboarding throughout the lifetime of your organization's use and includes the cybersecurity expertise you need to keep your practice, systems, reputation, data, people and patients safe.

It starts with onboarding, when you'll have the guidance of a Customer Success Manager and the support of CareStack's dedicated team throughout the process. It extends through CareStack's on-demand education resources, developed to enable your staff to stay updated on the latest software enhancements and share best practices.

You also benefit from automated backup and recovery. Regular data backups and robust recovery processes are in place to ensure business continuity in case of a cyber incident. Plus, you benefit from robust incident response protocols to ensure any breaches are swiftly contained and remediated. CareStack's incident management team is prepared to act immediately, minimizing the impact on your operations and ensuring a quick recovery.

*This white paper complements the Cybersecurity CareStack Straumann technical white paper, validating technical PMS aspects, such as data protection, policies and standards, proactive and reactive security, software supply chain, customer facing application security, compliance, and local privacy rules.

4. CARESTACK FOR A SECURE AND EFFICIENT DSO

Dental organizations can make financial and efficiency savings and simplify their IT estates by switching to the CareStack all-in-one practice management software.

At the same time, they gain significant cybersecurity benefits.

Data is more secure. Because CareStack is a cloud-based solution, security and patches are applied automatically. Backups can be automated too, enabling you to keep your last line of defense up to date with minimal effort too. There is less work for your IT teams – meaning fewer opportunities for them to overlook updates and less possibility of human error.

Enterprise-grade security tools, advanced user management and authentication and data encryption – both in transit and at rest – ensure the highest standards of cyber security. This is evidenced by CareStack's compliance with essential industry standards, including ISO 27001, HIPAA, GDPR, CCPA and SOC 2 Type I.

DSOs can practice a defense in depth approach with minimal effort, ensuring the best possible cybersecurity approach across their organization's key system and operational priorities.

*This white paper complements the Cybersecurity CareStack Straumann technical white paper, validating technical PMS aspects, such as data protection, policies and standards, proactive and reactive security, software supply chain, customer facing application security, compliance, and local privacy rules.

5. GET IN TOUCH

Request a product demo with our dedicated experts to understand how CareStack cyber-security benefits can be applied to your practice.

CURIOUS WHAT CARESTACK CAN BRING TO YOUR BUSINESS?

*CareStack is currently available in the United States, the United Kingdom, Singapore and Australia (Q4-2024).

*This white paper complements the Cybersecurity CareStack Straumann technical white paper, validating technical PMS aspects, such as data protection, policies and standards, proactive and reactive security, software supply chain, customer facing application security, compliance, and local privacy rules.

REFERENCES

1 Aspen Dental, "Notice of Cyber Security Incident" (December 2023): https://www.aspendental.com/data-security-incident. 2 Henry Schein, "Henry Schein Provides Information on Cybersecurity Incident" (October 2023): https://investor.henryschein.com/news-releases/news-release-details/henry-schein-provides-information-cybersecurity-incident. 3 Reuters, "Henry Schein cuts annual profit forecast as cyber-attack impact lingers" (August 2024): https://www.reuters.com/business/healthcare-pharmaceuticals/henry-schein-cuts-annual-profit-forecast-cyberattack-impact-lingers-2024-08-06/. 4 Forbes, "Cybersecurity Stats: Facts and Figures You Should Know" (August 2024): https://www.forbes.com/advisor/education/it-and-tech/cybersecurity-statistics/ 5 IBM, "Cost of a Data Breach Report 2024" (2024): https://www.ibm.com/reports/data-breach 6 National Institute of Standards and Technology (NIST), "Protecting Data from Ransomware and other data loss events": https://www.nccoe.nist.gov/sites/default/files/legacy-files/msp-protecting-data-extended.pdf 7 Statista, "Distribution of cyberattacks in healthcare industry worldwide from October 2021 to September 2022, by type" (September 2022): https://www.statista.com/statistics/1362863/cyber-attacks-on-healthcare-organizations-worldwide-by-type/ 8 Financial Times, "Cyber-attacks are one of the biggest threats facing healthcare systems" (January 2024): https://www.ft.com/content/77d54679-0915-4ce2-a42f-0c2b844da7ef 9 Expert Insights, "Healthcare Cyber Attack Statistics 2022: 25 Alarming Data Breaches You Should Know" (February 2024): https://expertinsights.com/insights/healthcare-cyber-attack-statistics/ 10 HIPAA Journal, "Global Healthcare Cyberattacks Increased by 74% in 2022" (January 2023): https://www.hipaajournal.com/global-healthcare-cyberattacks-increased-by-74-in-2022/ 11 NIST, "Ransomware Protection and Response" (May 2021): https://csrc.nist.gov/Projects/ransomware-protection-and-response 12 Proofpoint, "Proofpoint's 2023 State of the Phish Report Reveals Email-Based Attacks Dominated the Threat Landscape in 2022; Cyber Extortion Continues to Wreak Havoc Globally" (February 2023): https://www.proofpoint.com/uk/newsroom/press-releases/proofpoints-2023-state-phish-report-reveals-email-based-attacks-dominated 13 Forrester Research, "The Total Economic Impact of CareStack: Cost Savings and Business Benefits Enabled by CareStack" (October 2023): https://www.straumann.com/content/dam/media-center/straumann/en/documents/scientific-documentation/case-report/Forrester TEI_of_CareStack.pdf 14 HIPAA Journal, "Change Healthcare Reports Ransomware Data Breach to HHS" (July 2024): https://www.hipaajournal.com/change-healthcare-responding-to-cyberattack 15 TechTarget, "Change Healthcare cyberattack fallout continues" (May 2024): https://www.techtarget.com/healthtechsecurity/news/366594065/Change-Healthcare-cyberattack-fallout-continues

490.990/en/A/01 11/24

Distributor
Straumann USA, LLC
60 Minuteman Road
Andover, MA 01810
Phone 800/448 8168
Fax 978/747 2490
www.straumann.us

Legal Owner
Good Methods Global Inc
2940 Mallory Cir.
Kissimmee, FL 34747
Phone 832/545 1617

www.carestack.com

straumann