THE DIGITAL
Dental Record

September 3, 2019

To all DDS Safe clients:

With Labor Day now behind us, I'd like to provide another update on the Aug. 26 DDS Safe ransomware attack. Efforts to restore locked data continued over the holiday weekend, and PerCSoft reports that approximately 80% of the affected practices are now back to full or partial operation. Restoration and recovery work will continue in the coming days, with the hope of bringing all affected practices back online as soon as possible.

As I reported last week, The Digital Dental Record/DDS Safe and PerCSoft are in the process of fully investigating the scope of this attack and are working with the FBI's Cyber Crimes Task Force agents to determine the next steps. Additionally, we are working closely with a national, independent forensic investigation team to thoroughly investigate the incident, ensure it has been contained and prevent future attacks.

The DDR/DDS Safe phone lines continue to be fully staffed, and we have received additional questions from affected clients that I think would be beneficial to address for everyone. These include:

- **What if I still need help from PerCSoft?** If you are still finding issues that need to be addressed, please compile them into one email and send it to restore@percsoft.com. When emailing, please include your name, your practice's name, and direct contact information (name, phone and email) for your IT support person/company.

- **Will individual practices need to conduct their own investigations into the attack?** DDR/DDS Safe is working with the FBI's Cyber Crimes Task Force and a national, independent forensic team to conduct a thorough forensic investigation. We are hopeful that this investigation will uncover all the information needed to understand and remediate the full scope of the attack, and we will share the results of that investigation when we have information available. It is possible that investigation of each practice's environment may need to be done at a later date, but at this time, we are hopeful that is not necessary.

- **Has a data compromise been confirmed? Should I be notifying patients?** Determining whether personal, business and patient data was compromised is a top priority for investigators; however, it is still too early to confirm the extent of the attack and whether data was compromised (or merely locked). Notifications should not be made until a compromise is confirmed, and as of this email, no such compromise has been detected. If the investigation finds that data was compromised and notifications are required, DDR/DDS Safe and PerCSoft will immediately communicate that to impacted clients and assist them in complying with all applicable legal requirements.

We sincerely regret the inconvenience this situation has caused, and we remain committed to doing everything possible to support our clients through this difficult time. Please contact me at mroberts@profinsprog.com or 414.755.4170 if you have questions or need anything else.

Thank you for your time and patience.

Mara Roberts
The Digital Dental Record/DDS Safe

P.S. If you know an affected DDS Safe client who is not receiving email updates, please send their contact information to mroberts@profinsprog.com or have them call me at 414.755.4170.

September 3, 2019

To all Wisconsin Dental Association members:

With Labor Day now behind us, I'd like to provide another update on the Aug. 26 DDS Safe ransomware attack. Efforts to restore locked data continued over the holiday weekend, and PerCSoft reports that approximately 80% of the affected practices are now back to full or partial operation. Restoration and recovery work will continue in the coming days, with the hope of bringing all affected practices back online as soon as possible.

I reported last week that the WDAISC and PerCSoft are in the process of fully investigating the scope of this attack and are working with the FBI's Cyber Crimes Task Force agents to determine the next steps. Additionally, the WDAISC is working with a national, independent forensic investigation team to thoroughly investigate the incident, ensure it has been contained and prevent future attacks. The WDA and the ADA are monitoring the situation closely, helping to share information and doing what we can to support our members at this difficult time.

We continue to get questions about whether practice or patient data was accessed or compromised in the attack. In ransomware attacks, systems are encrypted and locked, but data is not always accessed or stolen. Determining whether information was accessed or stolen is a top priority for investigators; however, it is still too early to confirm the extent of the attack and whether a data breach occurred. If the investigation finds that data was compromised, WDAISC and PerCSoft will promptly communicate that information to clients and assist them in complying with all legal requirements for patient notifications and other steps that may apply.

I will plan to send another member update on Thursday, Sept. 5. If you have questions in the meantime, please contact WDAISC President Mara Roberts (mroberts@profinsprog.com – add "DDS Safe" to your subject line – or 414.755.4170).

As always, many thanks for your continued patience and support of the WDA.

Mark Paget
Executive Director

THE DIGITAL
Dental Record

August 30, 2019

To all DDS Safe customers:

As we head into the holiday weekend, I want to take a moment to update you on the recovery and restoration efforts that have been taking place since the ransomware attack on Monday, Aug. 26. Data recovery and system restoration is a slow and methodical process, and we deeply regret the frustration and inconvenience this has caused for you, your employees and your patients. We continue to be in extremely close contact with PerCSoft, which reports it has brought in additional support to assist with and expedite the restoration process. We do not have an exact number of practices that have been restored, but PerCSoft indicates they are making progress and will continue that work over the long weekend. DDS Safe will continue to take customer calls (414.755.4170 or 414.755.4196) over the holiday as well.

As the recovery process continues, we have received a few questions from clients that I thought would be helpful to address for the larger group:

- **Filing insurance claims:** Several clients have asked about insurance matters. We are advising all affected practices to contact their business insurance, cyber insurance and professional liability carriers to determine if coverage is available and start the claims process.

- **Communicating with patients about PHI and patient data:** We are currently in the process of fully investigating the scope of this ransomware attack and are working with the FBI's Cyber Crimes Task Force agents to determine the next steps we should take. We have not yet been able to determine whether any practice or patient data was accessed or compromised. In ransomware attacks, systems are encrypted and locked, but data is not always taken. It is too early in the investigation to confirm the extent of the attack and whether any data was compromised. If we learn that data was compromised, we will communicate that with you and comply with all legal requirements that may apply.

  Dentists have also asked if they should be proactively notifying patients of a potential compromise. At this time, we caution against making any notifications because, as set forth above, we simply do not know the scope of the attack. We do not want to inform patients that their information has been compromised if it has not been. Likewise, we do not want to make any assurances that no data was compromised as we may learn it has been. While we understand the process is unsettling, we ask that you allow us to complete our investigation prior to sending any notifications. We will have our investigation completed and will provide you with information within all legal reporting periods so that any required notifications can be made. If you would simply like to communicate with your patients given the business disruption, you may certainly do that, but please make it clear that the scope of the incident is still uncertain and that we are working hard to investigate the situation completely.

- **Responding to media inquiries:** We have heard from some clients who have been contacted by media regarding the situation. The decision to speak with media is yours; however, if you would like DDS Safe to respond to an inquiry, please contact Brenna Sadler at 414.755.4108 or bsadler@profservices.net.

We know this has been a difficult week, and we remain committed to doing everything possible to support you and your practice. Our team will be on duty throughout the holiday weekend; please call 414.755.4170 or 414.755.4196 if you have questions or need anything at all. We appreciate your patience and will work hard to regain your trust.

Mara Roberts
The Digital Dental Record/DDS Safe
414.755.4170
mroberts@profinsprog.com

WISCONSIN DENTAL ASSOCIATION

August 30, 2019

To all Wisconsin Dental Association members:

I want to thank those of you who took the time to respond to the WDA's Thursday, Aug. 29, email update on the DDS Safe situation. We received some very good questions, particularly from dentists who are receiving calls from patients worried about the security of their personal data. I thought it would be helpful to provide more information to help members address patient concerns, as well as share the latest update about restoration efforts heading into the holiday weekend.

As reported in yesterday's update, the WDAISC and PerCSoft are in the process of fully investigating the scope of this ransomware attack and are working with the FBI's Cyber Crimes Task Force agents to determine next steps. They have not yet been able to determine whether any practice or patient data was accessed or compromised. In ransomware attacks, systems are encrypted and locked, but data is not always taken. It is too early in the investigation to confirm the extent of the attack and whether any data was compromised. If the investigation finds that data was compromised, WDAISC and PerCSoft will communicate that to clients and comply with all legal requirements that may apply.

Dentists have also asked if they should be proactively notifying patients of a potential compromise. At this time, legal counsel urges caution against making any notifications because, as set forth above, the scope of the attack is just not known. We don't want to inform patients that information has been compromised if it hasn't, nor do we want to make assurances that data was not compromised if it was. While that process may be unsettling, it is important that the investigation be completed before sending out any notifications. We are assured the investigation will be finished and any information provided

within all legal reporting periods so that any required notifications can be made. If you would simply like to communicate with your clients about the business disruption, you may certainly do that, but please make it clear that the scope of the incident is still uncertain and that work is under way to investigate the situation completely.

As is often the case in situations like this one, we have heard several rumors making the rounds, including speculation about ransom paid to the hackers who orchestrated the attack. While we are unable to discuss details of the attack due to the ongoing investigation, I want to assure all members that the WDA has not paid a ransom of any type, and no member dues have been used in resolution of this situation.

We remain in close contact with the WDAISC and PerCSoft, which reports it has brought in additional support to assist with and expedite the restoration process. We do not have an exact number of practices that have been restored, but PerCSoft reports they are making continual progress on data recoveries. Work will continue over the long holiday weekend, and WDAISC staff will continue to take customer calls over the holiday as well.

I will plan to send another member update on Tuesday, Sept. 3. If you have questions in the meantime, please contact WDAISC President Mara Roberts (mroberts@profinsprog.com – add "DDS Safe" to your subject line – or 414.755.4170).

Thank you for your continued patience and support.

Mark Paget
Executive Director

THE DIGITAL Dental Record

"At 8:44 a.m. on Monday, Aug. 26, we learned that ransomware had been deployed on the remote management software our product uses to back up client data. Immediate action was taken to investigate and contain the threat. Our investigation and remediation efforts continue. Unfortunately, a number of practices have been and continue to be impacted by this attack.

"We deeply regret the frustration and inconvenience this has caused our clients, and we are working diligently with them and the software company to restore files as quickly and completely as possible. Restoration is a slow and methodical process that could take several more days to complete. Additionally, we are actively communicating with clients to answer questions, facilitate contact with appropriate insurance carriers and address other business concerns.

"The safety and security of the technology solutions we provide our clients is always our top priority. In conjunction with law enforcement, we are actively investigating the incident and will provide more information when we are able."

August 29, 2019

To all Wisconsin Dental Association members:

As we head into the holiday weekend, I want to take a moment to update you on an ongoing situation involving DDS Safe, a WDA endorsed product that is part of the WDA Insurance & Services Corp. At 8:44 a.m. on Monday, Aug. 26, WDAISC learned that ransomware had been deployed on the remote management software DDS Safe uses to back up client data. PerCSoft, the IT vendor for DDS Safe, took immediate action to contain the threat; however, roughly 400 practices around the country lost access to electronic files as a result of the virus.

PerCSoft assures us it is working to restore files as quickly and completely as possible, but restoration is a slow and methodical process that could take several days to complete. In the meantime, DDS Safe and the WDAISC are actively communicating with their clients to answer questions, facilitate contact with insurance carriers and address other business concerns. WDAISC is working diligently to fully investigate the situation and ensure it has been contained. It is also working with the Federal Bureau of Investigation's CyberCrime Unit as part of the investigation and response. We are in close communication with them and will provide updates when we can.

The safety, security and high quality of the endorsed products and services the WDA provides and recommends for our members is extremely important to us, and we are taking this matter very seriously. As WDAISC and PerCSoft work to return their clients to business, we are monitoring the situation, offering our assistance and fielding calls from members and the media. We are working closely with legal counsel, our insurers, the ADA and WDAISC leadership to ask questions, get answers and determine our next steps moving forward. At all times, what is good and right for our members, our members' livelihoods and the strength of the WDA is top of mind.

Our understanding is that only a small percentage of the affected practices are in Wisconsin, and that WDAISC and PerCSoft have been in touch with most of them. If you continue to have questions or would like to discuss this matter further, please feel free to reach out to WDAISC President Mara Roberts (mroberts@profinsprog.com – add "DDS Safe" to your subject line – or 414.755.4170). We will also provide updates on WDA.org as they are available.

Thank you for your patience and support during this very difficult situation.

Mark Paget
Executive Director