Peachtree Orthopedics alerts patients to cyberattack; third patient data breach in seven years

databreaches.net/peachtree-orthopedics-alerts-patients-of-cyberattack-third-patient-data-breach-in-seven-years/

Dissent May 20, 2023

An Atlanta clinic alerts patients to at least its third incident involving patient data in seven years.

Karakurt threat actors recently added Peachtree Orthopedics in Atlanta (Peachtree Orthopaedic Clinic, P.A.) to their leak site. As often seems to be the case with Karakurt listings, the date on Karakurt's post is somewhat confusing, and they make inconsistent claims about how much data they stole. In the screencap below, the date May 17 appears with "181 GB DATA" in red. In the post itself, which first appeared on or about May 12, they claim to have 194 GB of data, none of which has been leaked.

Image: DataBreaches.net

Finding no notice on their website, DataBreaches emailed Peachtree Orthopedics about the Karakurt listing on May 14 but received no reply. However, a re-check of their website today shows that they uploaded a statement dated May 12, 2023. The notice begins:

> On April 20, 2023, Peachtree Orthopedics determined an unauthorized party gained access to limited systems within our computer network. We immediately began an investigation, which included working with third-party specialists to determine the full nature and scope of the situation. We also notified law enforcement. While our investigation is ongoing, we cannot rule out unauthorized access to certain information for certain individuals. The type of information potentially affected varies by individual but may include name in combination with one or more of the following: address, date of birth, driver's license number, Social Security number, medical treatment/diagnosis information, treatment cost, financial account information, and health insurance claims/provider information.

Their description of potentially involved data is consistent with Karakurt's claim that the information they obtained includes "many lines with SSNs, almost 1000 of credit cards, other detailed personal information, medical records and tons of corporate data."

But Peachtree's statement does not confirm that any patient data was exfiltrated. It only says they can't rule out access "for certain individuals." Neither Peachtree nor Karakurt indicated how many patients had their PHI exfiltrated. And neither discloses the date of the attack. On April 20, Peachtree "determined" unauthorized access had occurred, but when did it begin, and when did Peachtree first discover abnormal activity on their network?

Peachtree's full notice can be read on its website. It does not offer patients any mitigation services at this point. It advises them on how to protect themselves but doesn't say how it will help them if their data was stolen. It reads, in part:

> Upon discovering this situation, we changed account passwords and implemented additional security measures to further protect information and reduce the risk of a similar situation occurring in the future. If you have questions about this situation or would like to determine if your information was potentially affected, please call 888-601-3774.

In a similar incident described below, Peachtree offered patients one year of credit monitoring and identity protection services. It would not be surprising if they do the same, or even more, in this case.

Previous Cyberattacks Involving Peachtree's Patient Data

This is the third cyberattack affecting Peachtree's patients in seven years that DataBreaches knows about.

The first incident was a massive hack and extortion attempt by thedarkoverlord in 2016, affecting 531,000 patients. In August 2016, DataBreaches' investigation into thedarkoverlord attacks on the medical sector revealed a compromise of an Illinois business associate had

been used to access several medical entities, including Peachtree Orthopedic. Peachtree eventually acknowledged the breach in October.

In its investigation into the incident, HHS's summary stated:

> Peachtree Orthopaedic Clinic, the covered entity, discovered that there had been an unauthorized intrusion into its computer system. It determined that the intruder may have been able to access the protected health information (PHI) of approximately 531,000 patients. The PHI included names, addresses, dates of birth, Social Security Numbers, and some clinical information.
>
> The covered entity retained a third party IT security firm to perform a forensic evaluation. It ended its relationship with the business associate that it concluded was the source of the compromise to its database. The covered entity also implemented several additional technical safeguards, including: a new intrusion detection system, improved its firewall, reset all of its user passwords, upgraded its anti-virus software, including additional monitoring of user activity, and implemented multi-factor authentication for remote users.
>
> As a result of OCR's investigation, Peachtree Orthopaedic Clinic also completed a new risk analysis.
>
> It provided breach notification to HHS, the affected individuals, the media, and on its website. OCR obtained assurances that the covered entity implemented the corrective actions outlined above.

In 2021, Peachtree Orthopedic suffered another breach involving patient data, and again it was due to a business associate. HHS's investigation into Peachtree's January 2022 report stated:

> Peachtree Orthopaedic Clinic, the covered entity, reported that its business associate (BA), experienced a ransomware attack that affected the electronic protected health information (ePHI) of 53,686 individuals. The ePHI involved included names, dates of service, and other treatment information. This breach has been consolidated into an existing compliance review of the BA.

The business associate was not named. From the limited information publicly available, that attack may not have been a direct attack on Peachtree's system but involved their patients' data on the associate's system.

Now there is a third cyberattack that appears to involve patient data. It is unclear whether any business associate was involved or the attackers gained direct access in another way. Given all the improvements made after the thedarkoverlord incident, how or where did

Peachtree's defenses fail if they did? There are numerous questions, and HHS will undoubtedly investigate what happened and how.

What Next?

Like thedarkoverlord before them, Karakurt does not lock or encrypt a victim's files or systems. They exfiltrate data, and then they try to extort the victim. DataBreaches does not know with certainty whether Peachtree Orthopedics paid thedarkoverlord not to dump all their patient data, but DataBreaches never saw any leak of all 530,000 patients' data. Was it leaked or sold privately, or did the attackers delete data because they got paid? DataBreaches does not know. Nor do we know whether Peachtree will pay Karakurt, but the fact that they are listed on Karakurt's site means that so far, there has been no agreement to pay.

DataBreaches will continue to monitor for updates to this incident.