# Report on Patient Privacy Volume 19, Number 10. October 10, 2019 Outsourcing IT? Here's How to Protect Your Organization

By Jane Anderson

It was a nightmare scenario[1] for dozens of dental clinics[2] in Oregon and Washington: They couldn't access patient records due to a ransomware attack, and they couldn't reach their information technology and security consultants, PM Consultants Inc., a small company in Portland, Oregon, that handled software updates, firewalls and data backups for the clinics.

As it turned out, PM Consultants itself was the epicenter of the July 3 attack. The ransomware was able to exploit security flaws at PM Consultants directly. An email from the company sent a week later urged clients to seek technical assistance elsewhere to recover their data, and a week after that, PM Consultants notified clients that it was closing its doors.

The ransomware attack and its aftermath underscore a major potential problem for smaller clinics and other health care entities that rely on outside contractors—managed service providers—to handle their information technology and security needs: How can they know if their IT consultants are themselves up to date and fully secure?

Cybercriminals, meanwhile, are finding it lucrative to target these contractors since they can open the digital doors to multiple downstream entities at once.

In another recent incident, for example, hackers in late August targeted PerCSoft, based in West Allis, Wisconsin, and blocked access to electronic files for 400 dental offices. In that case, the company paid the ransom and provided the decryption key to all practices. However, just as in the case of PM Consultants, the incident appears to have driven PerCSoft out of business.

So what can health care entities do to protect themselves? *Report on Patient Privacy* asked four security experts for their recommendations on how organizations can avoid finding themselves in a similar situation. Here's what they suggest.