



August 27, 2021

Dear Samaritan Center of Puget Sound Community,

We are writing to inform you of a recent security breach, which may have compromised your valued Personal Health Information (PHI). We would like to make sure you have the facts about what happened, what information was involved, and the steps we are taking to protect your information.

What Happened?

On the morning of July 19, 2021, we became aware that our main office building on Ravenna Blvd. had been broken into during the night. Burglars entered the facility by force, breaking windows, doors, and locks. Stolen items included an agency server, an office computer, tools, and audio/visual equipment.

The laptop and server were both stored and maintained behind two safeguards (physical locks and electronic passwords), consistent with HIPAA standards. However, their theft renders them vulnerable, each behind a single password. Consequently, PHI that was stored on the agency's network drives is at-risk.

What Information Was Involved?

The PHI stored on the agency's server spans a wide range of information, which, for you, could include: client names and dates of service, diagnoses and copies of charting content, addresses and phone numbers, copies of deposited checks, training videos, insurance information, social security numbers, and copies of billing statements.

It is important to clarify that the Valant EHR platform is cloud-based and not considered to be at-risk. Additionally, your therapist's email accounts are considered to be secure, with low-risk of breach. QuickBooks data was encrypted on the server, and archived data from our previously-held client database, Medisoft, was protected behind an additional password lock.

What We Are Doing

The Ravenna facility has been the subject of a number of attacks and break-ins during the last year. Throughout, we have increased security measures, to include added security alarm coverage, video cameras, and new locks. Since the latest incident, we continue to work toward heightened physical and electronic security. The new server is attached to the building in a new way, such that physical access (break-in) and theft are unlikely. Staff members have reset account passwords, and the new server passwords are reset.

Additionally, we are working with our IT associates to explore options for further encryption of network data going forward. At Samaritan Center, we take your privacy very seriously, and we will continue to look for ways to improve security.

We have also reported the incident to law enforcement authorities, and have requested investigation and pursuit of this criminal act.

What You Can Do

At this time, we are not aware of a known exposure (i.e., indications that someone has viewed any PHI), though a large amount of identifying information could be at risk. We will reach out if we have reason to believe such an exposure has occurred. As always, we encourage you to be watchful of your identity and let us know if you are contacted by anyone suspicious regarding your care at SCPS, or if you have reason to believe that your PHI has been accessed.

If you have any questions, please feel free to contact our HIPAA Privacy Officer at privacy@samaritanps.org or (206) 527-2266 x365.

Sincerely,

A handwritten signature in black ink that reads "Matthew Percy, Psy.D." with a stylized flourish at the end.

Matthew S. Percy, Psy.D.

Clinical Director
HIPAA Privacy Officer
Samaritan Center of Puget Sound
564 NE Ravenna Boulevard
Seattle, Washington 98115