Notice of Data Security Incident

On July 8, 2022, Cytometry Specialists, Inc. d/b/a CSI Laboratories ("CSI") learned that it had been the victim of a phishing attack after a single employee's individual mailbox was compromised. While CSI has no indication that any patient information has been misused, this notice explains the incident and outlines the measures we have taken in response.

What Happened?

Upon learning of the incident, we immediately took steps to isolate the affected email account and investigate the incident. We believe the access to a single employee mailbox occurred not to access patient information, but rather as part of an effort to commit financial fraud on other entities by redirecting CSI customer health care provider payments to an account posing as CSI using a fictitious email address. The invoices were not directly billed to patients. Thus, we believe that the malicious actor was seeking to divert invoice payments. However, as part of the investigation, on July 15, 2022, we determined that the unauthorized intruder acquired certain files from the affected employee mailbox, including documents that may have contained patient information. Since that time, we have been analyzing impacted files to understand what information may have been accessed or acquired by the malicious actor.

What Information Was Involved?

The impacted files were all related to invoices sent to CSI health care provider customers. The information in files differed from invoice to invoice, but generally, the files contained patient name and patient number (a unique number assigned to samples). Some impacted files contained more patient information, including date of birth and health insurance information. None of the files contained patient financial account information. Importantly, this incident was limited to a single CSI email inbox, and there was no impact on CSI's network or information systems. At this time, we have no facts suggesting that any of the patient information has been used and, in most cases, it will be very difficult, if not impossible, for anyone to further use the patient information that was accessed. Accordingly, we do not believe that you need to take any steps at this time to protect your information.

What We Are Doing

We engaged a well-known forensic investigation firm to identify the scope of the incident and took steps to further secure our email systems and increase employee awareness and training with respect to phishing attacks. The incident has been reported to law enforcement. We continue to closely monitor our network and information systems for unusual activity. We will continue to further improve security across our company networks and protect from unauthorized access or similar criminal activity in the future.

Contact

If you have concerns, please call CSI Client Services at 1-800-459-1185 between 9 am and 5 pm Eastern time.