Cancer & Hematology Centers of Western Michigan, P.C.
Notifies Individuals of Data Security Incident Involving Personal Information

Cancer & Hematology Centers of Western Michigan was the victim of a ransomware attack in late December that affected a portion of our database.

During this incident, unauthorized individuals may have accessed first and last names as well as other select pieces of information stored on the impacted database. For our patients, this may have included certain components of their health record. For our employees, Social Security numbers or bank information may have been accessed. We have no indication that anyone's data has been misused or further disclosed. Additionally, we have confirmed that there was no unauthorized access to the electronic medical records system.

Partnering with an outside team of respected IT and forensic experts, we worked to restore our systems and to ensure our data security. We also reported this incident to the FBI.

Working in tandem with our IT and forensic teams, we have conducted a thorough investigation to determine what occurred. The forensic analysis and investigation performed by a third-party IT security company could not identify any evidence showing unauthorized parties currently have access to our data or our system, or that there is risk for compromise to other systems.

We are now working with patients and employees who may have been affected. Out of an abundance of caution, we are offering credit monitoring at no charge. We also have established a toll-free hotline, 855.896.4446 to provide real-time answers for affected individuals.

Even one instance is one too many, and we have taken additional steps to strengthen our data security procedures. These include enhancing our security procedures, decommissioning several servers, mandating additional training, reviewing our policies and contracting with a third party for ongoing security monitoring.

Events of this nature are affecting an increasing number of companies in the U.S. and around the world. The federal government, law enforcement, and industry experts are working in tandem to address this activity.

We are sorry that this incident occurred and apologize to patients and team members who may have been affected. Safeguarding the personal information of our patients and employees is of the utmost importance to us. Since it is possible that we may have insufficient contact information for some individuals, we are posting this additional substitute notice as permitted by HIPAA, and this substitute notice will remain active for at least 90 days.