CHEMED – HIPAA SUBSTITUTE WEBSITE NOTICE POSTING

Center for Health Education, Medicine & Dentistry ("CHEMED") is providing notice of an incident that may affect the security of some of our patients' personal information. While there is currently no indicationthat patient information has been misused in relation to this incident, we are providing information on the incident, measures we have taken, and what you may do to better protect your personal information should you feel it appropriate to do so. On March 27, 2020, CHEMED began mailing written notice to patients it determined were impacted by this incident. CHEMED is posting notice of the incident here on our website because we were unable to identify a sufficient mailing address for some impacted patients.

What Happened?CHEMED uses a third-party Radiology imaging system (Konica) to send and store its studies to Radiologists to read. On December 10, 2019, CHEMED was notified that many Radiology providers across the Country had possibly been vulnerable to a potential opening which could allow unauthorized access to patient information. Working with outside computer forensics specialists, CHEMED commenced an investigation to determine the full extent of the issue. On February 20, 2020, the investigation determined that the vulnerability existed between July 28, 2015 and December 10, 2019.Although there were attempted unauthorized connections to the server from the public internet during that time period, CHEMED was unable to determine whether those connections were successful and specific patient records were actually subject to unauthorized access. CHEMED is therefore providing individuals with notice of this incident in an abundance of caution.

What Information Was Involved? The following types of patient information were determined to be at risk for possible unauthorized access: patient name, procedure date, patient date of birth, patient ID, exam ID, physician's name, and medical organization name(CHEMED).

What We Are Doing. We take this matter and the security and privacy of patient information in our care very seriously. After learning of this issue, Konica immediately took steps to correct the vulnerability and prevent unauthorized access to patient records in the future.

CHEMED is also mailingwritten notice directly to those patients determined to be affected for whom a sufficient mailing address could be identified. This notification includes information regarding steps they can take to protect against identity theft and fraud.

What You Can Do. Although at this time we have no indication to suggest the actual or attempted misuse of any patient information, we encourage you to review the below "Steps You Can Take to Protect Against Identity Theft and Fraud" for guidance on how to protect personal information.

For More Information. We understand you may have questions about this event that are not addressed in this notice, including whether you are an impacted patient. To ensure your questions are answered in a timely manner, we established a dedicated assistance line at 800-738-6028 which can be reached Monday through Friday from 8:00 a.m. to 5:00 p.m. Eastern Time.

We apologize for any inconvenience this incident may cause you and remain committed to the privacy and security of our patients' information.

Sincerely,

CHEMED

Privacy Safeguards

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements and Explanation of Benefits statements regularly, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
PO Box 9554	**P.O. Box 2000**	**PO Box 105788**
Allen, TX 75013	**Chester, PA 19016**	**Atlanta, GA 30348-5788**
1-888-397-3742	**1-888-909-8872**	**1-800-685-1111**
www.experian.com/freeze/center.html	**www.transunion.com/credit-freeze**	**www.equifax.com/personal/credit-report-services**

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.