August 26, 2020 – Assured Imaging ("Assured") is issuing notice of a recent data security event that may impact the confidentiality and security of personal information of certain Assured patients. Although Assured is unaware of any actual misuse of this information, we are providing information about the event, our response, and steps affected individuals may take to better protect against the possibility of identity theft and fraud, should affected individuals feel it is necessary to do so.

What Happened? On May 19, 2020, Assured learned that its electronic medical records system had become encrypted due to "ransomware" deployed by an unknown actor. Because the impacted systems contained patient information, Assured worked quickly to (1) restore access to the patient information so it could continue to care for patients without disruption and (2) investigate what happened and whether this incident resulted in any unauthorized access to, or theft of, patient information by the unknown actor.

Assured conducted an extensive investigation, with the assistance of third-party computer forensic specialists to determine the nature and scope of the incident. On July 1, 2020, the investigation confirmed Assured systems were accessible by an unknown actor between May 15, 2020 and May 17, 2020, and certain, limited data was exfiltrated from our systems. The investigation was unable to determine the full extent of information that was accessed by the unknown actor. In an abundance of caution, Assured performed a comprehensive review of all information stored in our systems at the time of incident to identify the individuals whose information may have been accessible to the unknown actor. We then worked to determine the identities and contact information for potentially impacted individuals.

What Information was Affected. The following types of patient information were present in the electronic medical records system and therefore potentially accessed and acquired by the unknown actor during this incident during the incident: full name, address, date of birth, patient ID, facility, treating clinician, medical history, service performed, and assessment of the service performed, including any recommendations on future testing. We are unaware that any of the information was misused by the unknown actor and Assured is providing this notice in an abundance of caution.

What We are Doing. Assured takes this incident and the security of your personal information seriously. Upon learning of this incident, we immediately took steps to restore our operations and further secure our systems. As part of our ongoing commitment to the privacy of personal information in our care, we are working to review our existing policies and procedures and to implement additional safeguards to further secure the information in our systems. Assured also notified the U.S. Department of Health and Human Services and other government regulators, as required.

What Affected Individuals Can Do. While we are unaware of any misuse of any personal information contained within the impacted system, individuals are encouraged to remain vigilant against incidents of identity theft by reviewing account statements and explanations of benefits for unusual activity and report any suspicious activity immediately to your insurance company, health care provider, or financial institution. Additional detail can be found below, in the *Steps You Can Take to Protect Your Information.*

For More Information. If you have additional questions, please call our dedicated assistance line at 866-938-0442, Monday through Friday (excluding U.S. holidays), during the hours of 8:00 a.m. to 5:00 p.m., Pacific Time (excluding U.S. holidays). You may also write to Assured at 7717 N. Hartman Lane, Tucson, AZ 85743

Steps You Can Take To Protect Your Information

While we are unaware of any misuse of the personal information in the affected system, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, 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**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348
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 9554	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.

For Maryland residents: The Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-410-528-8662, www.oag.state.md.us.

For North Carolina residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000, www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For New Mexico residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For Rhode Island residents: The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov, 1-401-274-4400. Under Rhode Island law, you have the right

to obtain any police report filed in regard to this incident. There are 4 Rhode Island residents impacted by this incident.

For New York residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

For Washington, D.C. residents: The Attorney General may be contacted at Office of the Attorney General, 441 4th Street, NW, Washington, DC 20001; (202) 727-3400; and www.oag@dc.gov.