Amanda Harvey
Office: (267) 930-1697
Fax: (267) 930-4771
Email: aharvey@mullen.law

4843 Colleyville Blvd, Suite 251-388
Colleyville, TX 76034

August 31, 2020

VIA E-MAIL

Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100
E-mail: securitybreach@atg.wa.gov

Re: Notice of Data Event

Dear Sir or Madam:

We represent Assured Imaging ("Assured") located at 7717 N. Hartman Lane, Tucson, AZ 85743, and are writing to notify your office of an incident that may affect the security of personal information relating to thirty-seven thousand seven hundred two (37,702) Washington residents. This notice may be supplemented if any new significant facts are learned subsequent to its submission. By providing this notice, Assured does not waive any rights or defenses regarding the applicability of Washington law or personal jurisdiction.

Nature of the Data Event

On May 19, 2020, Assured became aware that its electronic medical records system became encrypted due to "ransomware" deployed by an unknown actor. Because the server that was encrypted stored patient medical records, 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, personal information by the unknown actor.

Working with third-party computer forensic specialists, Assured was able to successfully restore the data contained on the impacted servers. On July 1, 2020, the forensic investigators confirmed there was exfiltration of limited amount of patient and employee information. Because of the uncertainty regarding which personal information was viewed or stolen by an unauthorized actor, it is notifying potentially affected individuals about this incident in an abundance of caution. On

or about August 11, 2020, Assured confirmed the identities of the individuals who may have had information affected by this incident.

Although the types of personal information potentially impacted varies by individual, the types of personal information potentially impacted for Washington residents includes: name, address, date of birth, Social Security number, driver's license number, bank account number, employee identification number, patient identification, facility, treating clinician, medical history, service performed, and assessment of the service performed, including any recommendations on future testing. There is no indication this information was misused by the unknown actor and Assured is providing this notice in an abundance of caution.

Notice to Washington Residents

On August 31, 2020, Assured began providing written notice of this incident to affected individuals, which includes thirty-seven thousand seven hundred two (37,702) Washington residents. Written notice was provided to affected individuals in substantially the same form as the letters attached here as ***Exhibit A*.** On August 26, 2020, Assured provided notice of this event on its website in substantially the same form as the notice attached here as ***Exhibit B***. Additionally, on August 27, 2020, Assured provided notice to prominent media outlets in Washington in substantially the same form as the notice attached here as ***Exhibit C.***

Other Steps Taken and To Be Taken

Upon discovering the potential unauthorized access to personal information as a result of the ransomware attack, Assured moved quickly to identify those that may be affected, put in place resources to assist them, and provide them with notice of this incident. Assured is also working to implement additional safeguards to protect the security of information in its systems.

Assured is providing written notice to those individuals who may be affected by this incident. This notice includes an offer of complimentary access to credit monitoring and identity restoration services through Experian for individuals with Social Security number impacted, and the contact information for a dedicated assistance line for potentially affected individuals to contact with questions or concerns regarding this incident. Additionally, Assured is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Assured is also providing written notice of this incident to other regulators, as necessary.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-1697.

Very truly yours,

Amanda Harvey of
MULLEN COUGHLIN LLC

ANH:zlg
Enclosure

EXHIBIT A

assuredimaging
women's wellness

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Re: Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

Assured Imaging ("Assured") is writing to inform you of a recent event that may impact the security of some of your information. Although we are unaware of any actual misuse of your information, we are providing you with information about the event, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you 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 and employee 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, personal 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, we 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 Involved. We determined the following types of information relating to you were present in the affected system and therefore potentially accessed by the unknown actor during this incident: name, address, date of birth, Social Security number, driver's license number, bank account number, and employee identification number. We are unaware that any of this information was misused by the unknown actor and Assured is providing this notice in an abundance of caution.

What We Are Doing. We take 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. While we are unaware of any misuse of your information as a result of this incident, we are offering you access to 12 months of credit monitoring and identity restoration services through Experian.

What You Can Do. You can find out more about how to protect against potential identity theft and fraud in the enclosed *Steps You Can Take to Help Protect Your Information.* We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements and explanations of benefits, and to monitor your credit reports for suspicious activity. You may also enroll in the complimentary credit monitoring services described above. Enrollment instructions are attached to this letter.

For More Information. If you have additional questions, please call our dedicated assistance line at 1-866-938-0442, 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.

We sincerely regret any inconvenience or concern this incident may cause.

Sincerely,

Kyle J. Dulock
Chief Privacy Officer
Assured Imaging

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enrollment Instructions

To help protect your identity, we are offering a complimentary one-year membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **<<b2b_text_1 (Date)>>** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: **https://www.experianidworks.com/3bcredit**
- Provide your **activation code**: **<<Member ID>>**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-877-288-8057 by **<<b2b_text_1 (Date)>>.** Be prepared to provide engagement number **<<b2b_text_2 (Engagement #)>>** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 1-877-288-8057. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

Monitor Your Accounts

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
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 160
Chester, PA 19016
1-888-909-8872
www.transunion.com/credit-freeze

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
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
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

Additional Information

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.

assuredimaging
women's wellness

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Re: Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

Assured Imaging ("Assured") is writing to inform you of a recent event that may impact the security of some of your information. Although we are unaware of any actual misuse of your information, we are providing you with information about the event, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you 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, we 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 Involved. We determined the following types of information relating to you were present in the electronic medical records system and therefore potentially accessed by the unknown actor during this 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 this information was misused by the unknown actor and Assured is providing this notice in an abundance of caution.

What We Are Doing. We take 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 You Can Do. You can find out more about how to protect against potential identity theft and fraud in the enclosed *Steps You Can Take to Help Protect Your Information.* We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements and explanations of benefits, and to monitor your credit reports for suspicious activity.

For More Information. If you have additional questions, please call our dedicated assistance line at 1-866-938-0442, 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.

We sincerely regret any inconvenience or concern this incident may cause.

Sincerely,

Kyle J. Dulock
Chief Privacy Officer
Assured Imaging

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts

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
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872
www.transunion.com/credit-freeze

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
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
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

Additional Information

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.

EXHIBIT B

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.

EXHIBIT C

Assured Imaging Provides Notice of Data Security Event

Tucson, Arizona August 27, 2020 – Today, Assured Imaging ("Assured") issued notice of a recent data security event that potentially affected the confidentiality of personal information related to certain patients.

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 Assured's 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 its systems at the time of incident to identify the individuals whose information may have been accessible to the unknown actor. Assured then worked to determine the identities and contact information for potentially impacted individuals.

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. Assured is unaware that any of the information was misused by the unknown actor and is providing this notice in an abundance of caution.

Assured is notifying potentially affected individuals by this posting, notification on its website, and by mailing letters to potentially affected individuals. For individuals seeking additional information regarding this incident, a dedicated toll-free assistance line has been established. Individuals may call the 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., Mountain Time.

Individuals can also find additional information on how they can protect their personal information as well as obtain additional resources on Assured's website https://www.assuredimaging.com/wp-content/uploads/2020/08/Rezolut-HIPAA-Website-Notice.pdf and in the letters they will receive by mail. As a precautionary measure, Assured encourages potentially affected individuals to remain vigilant against incidents of identity theft by reviewing account statements and explanations of benefits for unusual activity and reporting any suspicious activity immediately to their insurance company, health care provider, or financial institution.

Assured takes this incident and the security of the information in its care very seriously. As part of Assured's ongoing commitment to its patients, Assured is updating a range of privacy and security

safeguards designed to enhance the protections it has in place against ransomware and similar malicious attacks. Assured deeply regrets that this matter occurred and sincerely apologizes for any inconvenience or concern it may have caused.

# # #