Hoboken Radiology, LLC
Return to IDX
P.O Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

September 3, 2021

Re: Notice of Security Incident

Dear <<First Name>> <<Last Name>>:

Hoboken Radiology, LLC ("Hoboken") is writing to inform you of a event that may impact the privacy of some of your personal information. You are receiving this notice as part of our ongoing commitment to patient privacy. While we are unaware of any attempted or actual misuse of your information, we are providing you with information about the event, our response, and steps you may take to protect against any misuse of your information, should you feel it is necessary to do so.

What Happened? On November 3, 2020, Hoboken was informed of potentially suspicious activity involving its medical imaging server. Hoboken began investigating the activity with the assistance of third-party computer forensic specialists to determine if there had been any unauthorized access to its systems. That investigation is ongoing, but identified unauthorized connections between June 2, 2019 and December 1, 2020. The server on which suspicious activity was identified contained records related to Hoboken's patients. Therefore, in an abundance of caution, Hoboken is notifying patients that their information may have been at risk. The identified server does not contain patient payment card or financial information within its databases.

What Information Was Involved? The information contained on the server which may have been impacted by this incident includes your name, gender, date of birth, treatment date, referring physician, patient ID number, accession number, and image and description of image. The information at risk did not include any Social Security numbers, financial information, credit card information, or medical insurance information. Hoboken has no evidence your information was subject to actual or attempted misuse.

What We Are Doing. Hoboken takes this incident and the security of your personal information seriously. Upon discovery, we immediately launched an investigation and took steps to secure our systems. Hoboken worked diligently to investigate and respond to this incident and to identify and notify potentially impacted individuals. We are reviewing our policies, procedures, and processes related to storage of and access to personal information. Hoboken is also reporting this incident to relevant state and federal regulators as required.

What You Can Do. You can review the enclosed *Steps You Can Take to Help Protect Your Information* to learn helpful tips on steps you can take to protect against possible misuse should you feel it appropriate to do so. We also encourage you to review your financial and account statements, and explanation of benefits forms, and report all suspicious activity to the institution that issued the record immediately.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. We encourage you to contact IDX with any questions by calling 833-664-1994. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time.

We sincerely regret any inconvenience or concern this incident has caused.

Sincerely,

Hoboken Radiology

Steps You Can Take to Help Protect Your Information

Monitor Your Accounts.

To protect against the possibility of identity theft or other financial loss, we encourage you to remain vigilant, to review your account statements, and to monitor your credit reports for suspicious activity.

Credit Reports.

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.

Security Freeze.

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
1-888-397-3742	1-888-909-8872	1-888-298-0045
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

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	1-888-836-6351
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Additional Information.

You can further educate yourself regarding identity theft, and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission.

The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. 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); and TTY: 1-866-653-4261. Instances of known

or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC. You can also further educate yourself about placing a fraud alert or security freeze on your credit file by contacting the FTC or your state's Attorney General. This notice has not been delayed by a law enforcement investigation.

Maryland Residents: Office of the Attorney General of Maryland**,** Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023. **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 a 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. You can 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. **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/. **North Carolina Residents:** Office of the Attorney General of North Carolina**,** Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400, 877-566-7226 (toll free within NC). **Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392. **Rhode Island Residents:** Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 14 Rhode Island residents impacted by this incident. **Washington D.C. Residents:** the Office of Attorney General for the District of Columbia can be reached at: 400 6th Street NW Washington, D.C. 20001; 1-202-442-9828; https://oag.dc.gov. **All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

WEBSITE NOTICE

ABOUT THE DATA PRIVACY EVENT

On November 3, 2020, Hoboken Radiology LLC ("Hoboken") was informed of potentially suspicious activity on its computer network. Like many other medical providers, hospitals, and government agencies, Hoboken has unfortunately been the victim of unauthorized access to its imaging server. Hoboken, with the assistance of third-party computer forensic specialists, took steps to investigate the nature and scope of the incident. Hoboken is issuing this statement to provide additional details regarding what is known about the incident and the further steps it will be taking in response.

FREQUENTLY ASKED QUESTIONS

What Happened? On November 3, 2020, Hoboken was informed of potentially suspicious activity involving its medical imaging server. Hoboken began investigating the activity with the assistance of third-party computer forensic specialists to determine if there had been any unauthorized access to its systems. That investigation is ongoing, but identified unauthorized connections between June 2, 2019 and December 1, 2020. The server on which suspicious activity was identified contained records related to Hoboken's patients. Therefore, in an abundance of caution, Hoboken is notifying patients that some of their information may have been at risk. The identified server does not contain patient payment card or other financial or insurance information.

What Information Was Involved? The information contained on the server which may have been impacted by this incident included name, gender, date of birth, treatment date, referring physician, patient ID number, accession number, and image and description of image. The information at risk did not include any individual Social Security numbers, payment card or financial information, or medical insurance information. Hoboken has no evidence any information was subject to actual or attempted misuse.

What Is Hoboken Doing? Hoboken takes this incident and the security of personal information seriously. Upon discovery, Hoboken launched an investigation and took steps to secure its systems and investigate activity. Hoboken worked diligently to investigate and respond to this incident and to identify and notify potentially impacted individuals. Hoboken is also reviewing and enhancing existing policies, procedures, and processes related to storage of and access to personal information. Hoboken is notifying potentially impacted individuals so that they may take further steps to best protect their information, should they feel it is appropriate to do so. Hoboken is also reporting this incident to relevant state and federal regulators as required.

What Can Affected Individuals Do? While Hoboken has no evidence that any personal information was subject to actual or attempted misuse, it encourages anyone who thinks their information may have been impacted to monitor Explanation of Benefits forms, financial accounts, and notify their bank immediately if they detect unauthorized or unusual activity. You can also review the below *Steps You Can Take to Help Protect Your Information.*

For more information. If there are additional questions, Hoboken can be reached at 201-469-0550, via email to gberger@hobokenradiology.com or at 79 Hudson Street, Hoboken NJ, 07030.

The trust of our patients in Hoboken and its clinicians and staff are of the greatest importance to us, and we regret having to inform you that an incident such as this has occurred

Steps You Can Take to Help Protect Your Information

Hoboken apologizes for any inconvenience this may cause and remains committed to the privacy and security of all information it maintains.

Hoboken encourages individuals to remain vigilant against incidents of identity theft and fraud, to review account statements and explanation of benefits forms, and to monitor 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.

Individuals 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
1-888-397-3742	1-888-909-8872	1-888-298-0045
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, individuals will need to provide the following information:

1. 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.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

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	1-888-836-6351
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. 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); and TTY: 1-866-653-4261. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC. You can also further educate yourself about placing a fraud alert or security freeze on your credit file by contacting the FTC or your state's Attorney General. This notice has not been delayed by a law enforcement investigation.

Hoboken Radiology LLC – Notice of Data Privacy Event

Hoboken, NJ – June 1, 2021 – Hoboken Radiology LLC ("Hoboken") today is providing information about a recent event that may impact the privacy of some personal data related to current and former patients. Like many other medical providers, hospitals, and government agencies, Hoboken has unfortunately been the victim of unauthorized access to its imaging server.

What Happened? On November 3, 2020, Hoboken was informed of potentially suspicious activity involving its medical imaging server. Hoboken began investigating the activity with the assistance of third-party computer forensic specialists to determine if there had been any unauthorized access to its systems. That investigation is ongoing, but identified unauthorized connections between June 2, 2019 and December 1, 2020. The server on which suspicious activity was identified contained records related to Hoboken's patients. Therefore, in an abundance of caution, Hoboken is notifying patients that some of their information may have been at risk. The identified server does not contain patient payment card or other financial or insurance information.

What Information Was Involved? The information contained on the server which may have been impacted by this incident included name, gender, date of birth, treatment date, referring physician, patient ID number, accession number, and image and description of image. The information at risk did not include any individual Social Security numbers, payment card or financial information, or medical insurance information. Hoboken has no evidence any information was subject to actual or attempted misuse.

What Hoboken Is Doing. Hoboken takes this incident and the security of personal information seriously. Upon discovery, Hoboken immediately launched an investigation and took steps to secure its systems and investigate activity. Hoboken worked diligently to investigate and respond to this incident and to identify and notify potentially impacted individuals. Hoboken is also reviewing and enhancing existing policies, procedures, and processes related to storage of and access to personal information. Hoboken is notifying potentially impacted individuals so that they may take further steps to best protect their information, should they feel it is appropriate to do so. Hoboken is also reporting this incident to relevant state and federal regulators as required.

What You Can Do. While Hoboken has no evidence that any personal information was subject to actual or attempted misuse, it encourages anyone who thinks their information may have been impacted to monitor financial accounts and notify their bank immediately if they detect unauthorized or unusual activity. You can also review the below *Steps You Can Take to Help Protect Your Information.*

For more information. If there are additional questions, Hoboken can be reached at 201-469-0550, via email to gberger@hobokenradiology.com or at 79 Hudson Street, Hoboken NJ, 07030.

The trust of our patients in Hoboken and its clinicians and staff are of the greatest importance to us, and we regret having to inform you that an incident such as this has occurred.

Steps You Can Take to Help Protect Your Information

Hoboken encourages potentially impacted individuals to remain vigilant, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law, individuals with credit reports 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. The credit reporting agencies may be contacted as follows:

Experian	**TransUnion**	**Equifax**
PO Box 9554	P.O. Box 2000	PO Box 105788
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-888-909-8872	1-888-298-0045
www.experian.com	www.transunion.com	www.equifax.com/personal

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 also encourages those who discover that their information has been misused to file a complaint with them. 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); and TTY: 1-866-653-4261. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC. You can also further educate yourself about placing a fraud alert or security freeze on your credit file by contacting the FTC or your state's Attorney General.