ORTHOPEDIC ASSOCIATES

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

February 15, 2021

H5408-L04-0000004 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L04 SRS
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

[Re: Notice of Data Breach - CA Only]

Dear Sample A. Sample:

Orthopedic Associates of Hawaii, All Access Ortho and Specialty Suites d/b/a Minimally Invasive Surgery of Hawaii (collectively "the Practices") write to inform you of a recent event that may affect the security of some of your information. While we have no evidence of actual misuse of any information as a result of this event, this notice provides information about the event, our response, and resources available to you to help protect your information from possible misuse, should you feel it necessary to do so.

What Happened. On February 19, 2021, the Practices learned that their computer systems had become encrypted due to "ransomware" deployed by an unknown actor. Because the impacted systems contained patient information, we worked quickly to (1) restore access to the patient information so they could continue to care for patients without disruption, and (2) investigate what happened and whether this event resulted in any unauthorized access to, or theft of, patient information by the unknown actor.

We conducted an extensive investigation to determine the nature and scope of the event. On or around April 2, 2021, the investigation confirmed certain systems were accessible by an unknown actor between February 12, 2021 and February 19, 2021, and certain, limited data was downloaded. In an abundance of caution, we performed a comprehensive review of the information stored in our systems at the time of event to identify the individuals whose information may have been impacted. We then worked to confirm the identities and contact information for potentially affected individuals to provide notifications. This review was recently completed.

What Information was Affected. The following types of your information may have been present in the impacted systems during the event: full name, address, date of birth, medical treatment and diagnosis information, health insurance information, and for a limited number of individuals, Social Security number.

What We are Doing. We take this event and the security of your information seriously. Upon learning of this event, we immediately took steps to restore our operations and further secure our systems. As part of our ongoing commitment to the privacy of information in our care, we reviewed our existing policies and procedures and implemented additional administrative and technical safeguards to further secure the information in our systems. We also notified federal law enforcement, the U.S. Department of Health and Human Services, and other government regulators. While we are unaware of any misuse of your information as a result of this event, we are offering you access to [Credit Monitoring] months of complimentary credit monitoring and identity restoration services through Experian.

What You Can Do. As a precautionary measure, individuals are encouraged to remain vigilant against incidents of identity theft by reviewing account statements, credit reports, and explanations of benefits for unusual activity and to detect errors. We also encourage individuals to report any suspicious activity promptly to your insurance company, health care provider, or financial institution. Additional detail can be found in the *Steps You Can Take to Help Protect Your Information.* You may also enroll in the complimentary credit monitoring services described above. Enrollment instructions are enclosed with this letter.

For More Information. If you have additional questions, you may call our dedicated assistance line toll-free at (888) 397-0064, Monday through Friday from 6 a.m. to 8 p.m. Pacific, and Saturday and Sunday from 8 a.m. to 5 p.m. Pacific (excluding U.S. holidays). You may also write to the Practices at 1401 South Beretania Street, Suite 750, Honolulu, HI 96814.

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

Sincerely,

Jessica Dew

Jessica Dew
Nurse Manager
The Practices

Steps You Can Take To Help Protect Your Information

Enroll in Credit Monitoring

To help protect your identity, we are offering a complimentary [Credit Monitoring]-month 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**: **April 30, 2022** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- Provide your **activation code**: **ABCDEFGHI**

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 (888) 397-0064 by **April 30, 2022**. Be prepared to provide engagement number **ENGAGE#** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR [Credit Monitoring]-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 file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents 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 (888) 397-0064. 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 [Credit Monitoring] months 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.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-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 three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit 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 credit 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 credit freeze on your credit report. To request a security freeze, you 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. Addresses for the prior two to 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.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may 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. 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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th St. NW Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202;1-888-743-0023; and www.oag.state.md.us.

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

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 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 13 Rhode Island residents impacted by this event.

ORTHOPEDIC ASSOCIATES

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

February 15, 2021

H5408-L01-0000001 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01 ADULT
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

[Re: Notice of Data Breach - CA Only]

Dear Sample:

Orthopedic Associates of Hawaii, All Access Ortho and Specialty Suites d/b/a Minimally Invasive Surgery of Hawaii (collectively "the Practices") write to inform you of a recent event that may affect the security of some of your information. While we have no evidence of actual misuse of any information as a result of this event, this notice provides information about the event, our response, and resources available to you to help protect your information from possible misuse, should you feel it necessary to do so.

What Happened. On February 19, 2021, the Practices learned that their computer systems had become encrypted due to "ransomware" deployed by an unknown actor. Because the impacted systems contained patient information, we worked quickly to (1) restore access to the patient information so they could continue to care for patients without disruption, and (2) investigate what happened and whether this event resulted in any unauthorized access to, or theft of, patient information by the unknown actor.

We conducted an extensive investigation to determine the nature and scope of the event. On or around April 2, 2021, the investigation confirmed certain systems were accessible by an unknown actor between February 12, 2021 and February 19, 2021, and certain, limited data was downloaded. In an abundance of caution, we performed a comprehensive review of the information stored in our systems at the time of event to identify the individuals whose information may have been impacted. We then worked to confirm the identities and contact information for potentially affected individuals to provide notifications. This review was recently completed.

What Information was Affected. The following types of your information were present in the impacted systems during the event: full name, address, [Data Elements].

What We are Doing. We take this event and the security of your information seriously. Upon learning of this event, we immediately took steps to restore our operations and further secure our systems. As part of our ongoing commitment to the privacy of information in our care, we reviewed our existing policies and procedures and implemented additional administrative and technical safeguards to further secure the information in our systems. We also notified federal law enforcement, the U.S. Department of Health and Human Services, and other government regulators. While we are unaware of any misuse of your information as a result of this event, we are offering you access to [Credit Monitoring] months of complimentary credit monitoring and identity restoration services through Experian.

What You Can Do. As a precautionary measure, individuals are encouraged to remain vigilant against incidents of identity theft by reviewing account statements, credit reports, and explanations of benefits for unusual activity and to detect errors. We also encourage individuals to report any suspicious activity promptly to your insurance company, health care provider, or financial institution. Additional detail can be found below in the *Steps You Can Take to Help Protect Your Information.* You may also enroll in the complimentary credit monitoring services described above. Enrollment instructions are enclosed with this letter.

For More Information. If you have additional questions, you may call our dedicated assistance line toll-free at (888) 397-0064, Monday through Friday from 6 a.m. to 8 p.m. Pacific, and Saturday and Sunday from 8 a.m. to 5 p.m. Pacific (excluding U.S. holidays). You may also write to the Practices at 1401 South Beretania Street, Suite 750, Honolulu, HI 96814.

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

Sincerely,

Jessica Dew

Jessica Dew
Nurse Manager
The Practices

Steps You Can Take To Help Protect Your Information

Enroll in Credit Monitoring

To help protect your identity, we are offering a complimentary [Credit Monitoring]-month 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**: **April 30, 2022** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- Provide your **activation code**: **ABCDEFGHI**

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 (888) 397-0064 by **April 30, 2022**. Be prepared to provide engagement number **ENGAGE#** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR [Credit Monitoring]-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 file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents 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 (888) 397-0064. 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 [Credit Monitoring] months 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.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-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 three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit 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 credit 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 credit freeze on your credit report. To request a security freeze, you 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. Addresses for the prior two to 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.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may 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. 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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th St. NW Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202;1-888-743-0023; and www.oag.state.md.us.

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

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 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 13 Rhode Island residents impacted by this event.

February 15, 2022 – Orthopedic Associates of Hawaii, All Access Ortho and Specialty Suites d/b/a Minimally Invasive Surgery of Hawaii (collectively "the Practices") are issuing notice of a data security event that may impact the confidentiality and security of information related to certain patients. Although the Practices are 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 appropriate to do so.

What Happened. On February 19, 2021, the Practices learned that their computer systems had become encrypted due to "ransomware" deployed by an unknown actor. Because the impacted systems contained patient information, the Practices worked quickly to restore access to the patient information so they could continue to care for patients without disruption and investigate what happened and whether the event resulted in any unauthorized access to, or theft of, patient information by the unknown actor.

The Practices conducted an extensive investigation to determine the nature and scope of the event. On or around April 2, 2021, the investigation confirmed the Practices' systems were accessible by an unknown actor between February 12, 2021 and February 19, 2021, and certain, limited data was exfiltrated from our systems. In an abundance of caution, the Practices undertook a comprehensive review of the information stored in our systems at the time of event to identify the individuals whose information may have been viewed or taken by the unknown actor. The Practices recently completed this review and provided notice to potentially affected individuals via written letter.

What Information was Affected. The following types of patient information were present in the impacted systems and therefore potentially accessed and acquired by the unknown actor during the event: full name, address, date of birth, driver's license number, health insurance information, medical information, including treatment and diagnosis information, financial account information, and payment card information. For a limited number of individuals, Social Security number may have also been impacted. We are unaware that any of the information was actually misused or disseminated by the unknown actor.

What We are Doing. The Practices take this event and the security of your information seriously. Upon learning of this event, 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 reviewed our existing policies and procedures and implemented additional administrative and technical safeguards. The Practices also notified federal law enforcement, the U.S. Department of Health and Human Services, and other government regulators.

What Affected Individuals Can Do. As a precautionary measure, individuals are encouraged to remain vigilant against incidents of identity theft by reviewing account statements, and explanations of benefits, and credit reports for unusual activity and to detect errors. Any suspicious activity should be promptly reported to your insurance company, health care provider, or financial institution. Additional detail can be found below in the *Steps You Can Take to Help Protect Your Information.*

For More Information. If you have additional questions, you may call our dedicated assistance line at (888)397-0064, Monday through Friday (excluding U.S. holidays), during the hours of 6:00 a.m. to 8:00 p.m., Pacific Standard Time, and Saturday and Sunday from 8:00 a.m. to 5:00 p.m., Pacific Standard Time. You may also write to the Practices at 1401 South Beretania Street, Suite 750, Honolulu, HI 96814.

Steps You Can Take To Help Protect Your Information

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-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 three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit 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 credit 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 credit freeze on your credit report. To request a security freeze, you 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. Addresses for the prior two to 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.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit

reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may 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. 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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 4006th St. NW Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202;1-888-743-0023; and www.oag.state.md.us.

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

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this event.

OAH – HIPAA Media Notice - Updated

Orthopedic Associates of Hawaii, All Access Ortho and Specialty Suites d/b/a Minimally Invasive Surgery of Hawaii Provides Notice of Data Security Event

Honolulu, Hawaii February 15, 2022 – Today, Orthopedic Associates of Hawaii, All Access Ortho and Specialty Suites d/b/a Minimally Invasive Surgery of Hawaii (collectively "the Practices") issued notice of a data security event that potentially affected the confidentiality of information related to certain patients.

On February 19, 2021, the Practices learned that their computer systems had become encrypted due to "ransomware" deployed by an unknown actor. Because the impacted systems contained patient information, the Practices worked quickly to restore access to the patient information so they could continue to care for patients without disruption and investigate what happened and whether this event resulted in any unauthorized access to, or theft of, patient information by the unknown actor.

The Practices conducted an extensive investigation to determine the nature and scope of the event. On or around April 2, 2021, the investigation confirmed the Practices' systems were accessible by an unknown actor between February 12, 2021 and February 19, 2021, and certain, limited data was exfiltrated from the Practice's systems. In an abundance of caution, the Practices conducted a comprehensive review of the information stored in their systems at the time of event to identify the individuals whose information may have been viewed or taken by the unknown actor. The Practices recently completed this review and worked to determine the identities and contact information for potentially affected individuals and provided notice via written letter.

The following types of patient information were present in the impacted systems and therefore potentially accessed and acquired during the event: full name, address, date of birth, driver's license number, health insurance information, medical information, including treatment and diagnosis information, financial account information, and payment card information. For a limited number of individuals, Social Security number may have also been impacted. The Practices are unaware that any of the information was misused or disseminated by the unknown actor.

The Practices are notifying potentially affected individuals by this posting, notification on their websites, and by mailing letters to potentially affected individuals. The Practices also notified federal law enforcement and other government regulators. For individuals seeking additional information regarding this event, a dedicated toll-free assistance line has been established. Individuals may call the assistance line at (888)397-0064, Monday through Friday (excluding U.S. holidays), during the hours of 6:00 a.m. to 8:00 p.m., Pacific Standard Time, and Saturday and Sunday from 8:00 a.m. to 5:00 p.m., Pacific Standard Time.

Individuals can also find additional information on how they can help protect their information as well as obtain additional resources on the Practices' websites [URLs for website notices]. As a precautionary measure, the Practices encourage potentially affected individuals to remain vigilant against incidents of identity theft by reviewing account statements, explanations of benefits, and credit reports for unusual activity and to detect errors. Any suspicious activity should be promptly reported to their insurance company, health care provider, or financial institution.

The Practices takes this event and the security of the information in their care very seriously. As part of the Practices' ongoing commitment to its patients, the Practices updated a range of privacy and security safeguards designed to enhance the protections they have in place against ransomware and similar malicious attacks.

# # #