

Buffalo
Chicago
New York
Raleigh
Washington D.C.



www.octillolaw.com

May 14, 2025

VIA EMAIL

Office of the Attorney General
1125 Washington Street SE
P.O. Box 40100
Olympia, WA 98504-0100

Dear Sir or Madam:

On behalf of Kitsap Mental Health Services (“KMHS”), whose office is located at 5455 Almira Dr. NE, Bremerton, WA 98311, and pursuant to Wash. Rev. Code § 19.255.010 *et seq.*, this letter provides supplemental information regarding a data security incident that was reported to this office on December 16, 2024. By providing notice and supplemental information, KMHS does not waive any rights or defenses regarding the applicability of Washington law or personal jurisdiction.

KMHS is a not-for-profit organization providing a full range of inpatient, outpatient, and residential behavioral health services for children, adults, and families. On October 17, 2024, during routine monitoring of systems, KMHS detected suspicious activity on its business network. KMHS immediately began an investigation and took steps to contain and remediate the situation, including by changing passwords, deploying tools for increased monitoring, reporting to law enforcement, and engaging data security and privacy experts to assist. The investigation has found evidence that on September 17, 2024, and between October 8, 2024 and October 19, 2024, an unauthorized actor accessed some KMHS systems. There is currently no evidence of identity theft or fraud in connection with this incident.

On December 16, 2024, KMHS provided notice to the Department of Health and Human Services Office for Civil Rights, and published substitute notice on its website and via media notice, in compliance with the Health Insurance Portability and Accountability Act (“HIPAA”) in order to notify potentially affected individuals while the investigation to identify the data pertaining to specific individuals was still ongoing.

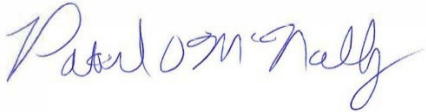
KMHS has since completed its investigation and determined that 57,818 Washington residents were affected. KMHS has identified that the following types of information may have been impacted: Name, Date of Birth, Social Security Number, Medical Record Number (MRN), Patient Account Number (PAN), Health Insurance Account Member Number, Medical Diagnosis Information, Medical Treatment/Procedure Information, Clinical Information, Prescription Information, Provider Location, Provider Name. Beginning on May 14, 2025, letters will be mailed to affected individuals for whom

complete addresses are available. A sample copy of that individual notice is attached for your review. KMHS has also posted an updated notice on its website.

Please feel free to contact me with any questions at (716) 898-2102 or pmcnally@octillolaw.com.

Sincerely,

OCTILLO

A handwritten signature in blue ink that reads "Patrick D. McNally". The signature is written in a cursive, flowing style.

Patrick D. McNally, Esq.
Certified Information Privacy Professional, United States (CIPP/US)

Encl.



May 14, 2025

VIA U.S. MAIL

[NAME]

[ADDRESS]

[CITY, STATE, ZIP]

Dear [NAME],

We are writing to inform you that Kitsap Mental Health Services (“KMHS” or “we”) experienced a data incident in October 2024 (the “Incident”) that potentially involved your personal information (“Information”). This letter provides you with information about this Incident, our response, and information on where to direct your questions. Additionally, although we are unaware of any misuse of your Information or fraud in relation to the Incident, as a precaution we have also provided steps you can take to protect your Information, including the ability to enroll in credit monitoring services that we are offering free of charge for twelve (12) months.

What Happened?

On October 17, 2024, during routine monitoring of our systems, KMHS detected suspicious activity in our business network. We immediately began an investigation and took steps to contain and remediate the situation, including by changing passwords, deploying tools for increased monitoring, reporting to law enforcement, and engaging data security and privacy experts to assist.

The investigation found evidence that on September 17, 2024, and between October 8, 2024 and October 19, 2024, an unauthorized actor accessed some KMHS systems and downloaded data, which included your Information. There is currently no evidence of identity theft or fraud in connection with this Incident.

What Information Was Involved?

We determined that the following types of Information may have been impacted as a result of this Incident: Name, <Breached Elements>.

What We Are Doing.

Upon becoming aware of the Incident, we immediately implemented measures to further improve the security of our systems and practices, including implementing endpoint detection and response monitoring. After determining that an unauthorized actor gained access to our systems, we immediately began analyzing the information involved to confirm the identities of potentially affected individuals and notify them. The KMHS team has worked diligently to complete our investigation, add further technical safeguards to our existing protections, and bring systems back online as quickly and securely

as possible. We continue to work with leading privacy and security firms to aid in our response, and we reported this Incident to relevant government agencies.

What Can You Do?

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for twelve (12) months. While identity restoration assistance is immediately available to you, we also encourage you to activate the complimentary twelve (12) month membership to Experian IdentityWorks and its fraud detection tools. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- You must **enroll by July 31, 2025** (Your code will not work after this date).
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>.
- Provide your **activation code**: <<Activation Code>>.

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this Incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [REDACTED] by July 31, 2025. Be prepared to provide engagement number [REDACTED] as proof of eligibility for the Identity Restoration services by Experian.

It is always recommended that you remain vigilant, regularly monitor free credit reports, review account statements, and report any suspicious activity to financial institutions. Please also review the "Additional Resources" section included with this letter, which outlines other resources you can utilize to protect your Information.

For More Information.

We take this Incident and the security of information in our care seriously. If you have questions related to credit monitoring services, please contact Experian at the number provided above. If you have additional questions, you may call our toll-free assistance line at [REDACTED] Monday through Friday from 6:00 a.m. to 6:00 p.m. Pacific Time (excluding U.S. holidays).

Sincerely,

Nadine Randklev
Chief Compliance Officer

Encl.

ADDITIONAL RESOURCES

Contact information for the three (3) nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every twelve (12) months from each of the three (3) nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one (1) or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by calling one (1) of the three (3) nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Security Freeze. You may obtain a security freeze on your credit report, free of charge, to protect your privacy and confirm that credit is not granted in your name without your knowledge. You may also submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report, free of charge, or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place.

To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three (3) credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for them as well): (1) full name, with middle initial, and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

Protecting Medical Information.

If you are concerned about protecting your medical information, the following practices can provide additional safeguards to protect against medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.

- Review your “explanation of benefits statement” which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

For Alabama Residents: You may contact the Attorney General’s Office for the State of Alabama, Consumer Protection Division, 501 Washington Avenue, Montgomery, AL 36104, www.alabamaag.gov, 1-800-392-5658.

For California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225. This notification was not delayed as a result of any law enforcement investigation.

For Colorado Residents: You can obtain information from the federal trade commission and the credit reporting agencies about fraud alerts and security freezes.

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For District of Columbia Residents: You can obtain information about steps to take to avoid identity theft from the Federal Trade Commission (contact information above) and The District of Columbia Office of the Attorney General, 400 6th Street NW, Washington, D.C. 20001, consumer.protection@dc.gov, <https://oag.dc.gov/>, (202) 737-3400.

For Illinois Residents: You can obtain information from the credit reporting agencies and the Federal Trade Commission about fraud alerts and security freezes (contact information above). You may contact the Illinois Office of the Attorney General, 100 West Randolph Street, Chicago, IL 60601, https://illinoisattorneygeneral.gov/about/email_ag.jsp, 1-800-964-3013.

For Iowa Residents: You may contact the Iowa Office of the Attorney General, 1305 E. Walnut Street, Des Moines, IA 50319, consumer@ag.iowa.gov; www.iowattorneygeneral.gov, 1-888-777-4590.

For Kansas Residents: You may contact the Kansas Office of the Attorney General, Consumer Protection Division, 120 SW 10th Ave, 2nd Floor, Topeka, KS 66612-1597, <https://ag.ks.gov/>, 1-800-432-2310.

For Kentucky Residents: You may contact the Kentucky Office of the Attorney General, Consumer Protection Division, 1024 Capital Center Drive, Suite 200, Frankfort, Kentucky 40601, www.ag.ky.gov, 1-800-804-7556.

For Maryland Residents: You may obtain information about steps you can take to avoid identity theft from the Federal Trade Commission (contact information above) and the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov, 1-888-743-0023.

For Massachusetts Residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html.

For Minnesota Residents: You may contact the Minnesota Office of the Attorney General, 445 Minnesota Street, Suite 1400, St. Paul, MN 55101, www.ag.state.mn.us, 1-800-657-3787.

For Missouri Residents: You may contact the Missouri Office of the Attorney General, Consumer Protection, 207 W. High St., P.O. Box 899, Jefferson City, MO 65102, www.ago.mo.gov, 1-800-392-8222.

For Nevada Residents: You may contact the Nevada Office of the Attorney General, Bureau of Consumer Protection, 100 N. Carson St, Carson City, NV 89701, www.ag.nv.gov, 1-702-486-3132.

For New Mexico Residents: Consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their 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 consumers’ files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit “prescreened” offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their 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: You may obtain information regarding security breach response and identity theft prevention and protection information from the Federal Trade Commission (contact information above) and the New York Office of the Attorney General, Office of the Attorney General, The Capitol, Albany, NY 12224-0341, <https://ag.ny.gov>, 1-800-771-7755.

For North Carolina Residents: You may obtain information about preventing identity theft from the Federal Trade Commission (contact information above) and the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Main Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7266 or 1-919-716-6400.

For Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392.

For Pennsylvania Residents: You may contact the Pennsylvania Office of the Attorney General, Bureau of Consumer Protection, 15th Floor, Strawberry Square, Harrisburg, PA 17120, www.attorneygeneral.gov, 1-800-441-2555.

For Rhode Island Residents: You may contact the Rhode Island Office of the Attorney General, Consumer Protection Division, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 1-401-274-4400.

For Texas Residents: You may contact the Texas Office of the Attorney General, Office of the Attorney General, PO Box 12548, Austin, TX 78711-2548, www.texasattorneygeneral.gov, 1-800-621-0508.

For Wyoming Residents: This notification was not delayed as a result of any law enforcement investigation.

Reporting of identity theft and obtaining a police report. You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

For Iowa Residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts Residents: You have the right to obtain a police report if you are a victim of identity theft.

For North Carolina Residents: You are advised to report any suspected identity theft to law enforcement or to the North Carolina Attorney General.

For Oregon Residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

<<Variable data 5>>>

Buffalo
Chicago
New York
Raleigh
Washington D.C.



www.octillolaw.com

May 14, 2025

VIA EMAIL

Office of the Attorney General
1125 Washington Street SE
P.O. Box 40100
Olympia, WA 98504-0100

Dear Sir or Madam:

On behalf of Kitsap Mental Health Services (“KMHS”), whose office is located at 5455 Almira Dr. NE, Bremerton, WA 98311, and pursuant to Wash. Rev. Code § 19.255.010 *et seq.*, this letter provides supplemental information regarding a data security incident that was reported to this office on December 16, 2024. By providing notice and supplemental information, KMHS does not waive any rights or defenses regarding the applicability of Washington law or personal jurisdiction.

KMHS is a not-for-profit organization providing a full range of inpatient, outpatient, and residential behavioral health services for children, adults, and families. On October 17, 2024, during routine monitoring of systems, KMHS detected suspicious activity on its business network. KMHS immediately began an investigation and took steps to contain and remediate the situation, including by changing passwords, deploying tools for increased monitoring, reporting to law enforcement, and engaging data security and privacy experts to assist. The investigation has found evidence that on September 17, 2024, and between October 8, 2024 and October 19, 2024, an unauthorized actor accessed some KMHS systems. There is currently no evidence of identity theft or fraud in connection with this incident.

On December 16, 2024, KMHS provided notice to the Department of Health and Human Services Office for Civil Rights, and published substitute notice on its website and via media notice, in compliance with the Health Insurance Portability and Accountability Act (“HIPAA”) in order to notify potentially affected individuals while the investigation to identify the data pertaining to specific individuals was still ongoing.

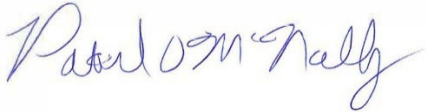
KMHS has since completed its investigation and determined that 56,981 Washington residents were affected. KMHS has identified that the following types of information may have been impacted: Name, Date of Birth, Social Security Number, Medical Record Number (MRN), Patient Account Number (PAN), Health Insurance Account Member Number, Medical Diagnosis Information, Medical Treatment/Procedure Information, Clinical Information, Prescription Information, Provider Location, Provider Name. Beginning on May 14, 2025, letters will be mailed to affected individuals for whom

complete addresses are available. A sample copy of that individual notice is attached for your review. KMHS has also posted an updated notice on its website.

Please feel free to contact me with any questions at (716) 898-2102 or pmcnally@octillolaw.com.

Sincerely,

OCTILLO

A handwritten signature in blue ink that reads "Patrick D. McNally". The signature is written in a cursive, flowing style.

Patrick D. McNally, Esq.
Certified Information Privacy Professional, United States (CIPP/US)

Encl.



May 14, 2025

VIA U.S. MAIL

[NAME]

[ADDRESS]

[CITY, STATE, ZIP]

Dear [NAME],

We are writing to inform you that Kitsap Mental Health Services (“KMHS” or “we”) experienced a data incident in October 2024 (the “Incident”) that potentially involved your personal information (“Information”). This letter provides you with information about this Incident, our response, and information on where to direct your questions. Additionally, although we are unaware of any misuse of your Information or fraud in relation to the Incident, as a precaution we have also provided steps you can take to protect your Information, including the ability to enroll in credit monitoring services that we are offering free of charge for twelve (12) months.

What Happened?

On October 17, 2024, during routine monitoring of our systems, KMHS detected suspicious activity in our business network. We immediately began an investigation and took steps to contain and remediate the situation, including by changing passwords, deploying tools for increased monitoring, reporting to law enforcement, and engaging data security and privacy experts to assist.

The investigation found evidence that on September 17, 2024, and between October 8, 2024 and October 19, 2024, an unauthorized actor accessed some KMHS systems and downloaded data, which included your Information. There is currently no evidence of identity theft or fraud in connection with this Incident.

What Information Was Involved?

We determined that the following types of Information may have been impacted as a result of this Incident: Name, <Breached Elements>.

What We Are Doing.

Upon becoming aware of the Incident, we immediately implemented measures to further improve the security of our systems and practices, including implementing endpoint detection and response monitoring. After determining that an unauthorized actor gained access to our systems, we immediately began analyzing the information involved to confirm the identities of potentially affected individuals and notify them. The KMHS team has worked diligently to complete our investigation, add further technical safeguards to our existing protections, and bring systems back online as quickly and securely

as possible. We continue to work with leading privacy and security firms to aid in our response, and we reported this Incident to relevant government agencies.

What Can You Do?

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for twelve (12) months. While identity restoration assistance is immediately available to you, we also encourage you to activate the complimentary twelve (12) month membership to Experian IdentityWorks and its fraud detection tools. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- You must **enroll by July 31, 2025** (Your code will not work after this date).
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>.
- Provide your **activation code**: <<Activation Code>>.

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this Incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [REDACTED] by July 31, 2025. Be prepared to provide engagement number [REDACTED] as proof of eligibility for the Identity Restoration services by Experian.

It is always recommended that you remain vigilant, regularly monitor free credit reports, review account statements, and report any suspicious activity to financial institutions. Please also review the "Additional Resources" section included with this letter, which outlines other resources you can utilize to protect your Information.

For More Information.

We take this Incident and the security of information in our care seriously. If you have questions related to credit monitoring services, please contact Experian at the number provided above. If you have additional questions, you may call our toll-free assistance line at [REDACTED] Monday through Friday from 6:00 a.m. to 6:00 p.m. Pacific Time (excluding U.S. holidays).

Sincerely,

Nadine Randklev
Chief Compliance Officer

Encl.

ADDITIONAL RESOURCES

Contact information for the three (3) nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every twelve (12) months from each of the three (3) nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one (1) or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by calling one (1) of the three (3) nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Security Freeze. You may obtain a security freeze on your credit report, free of charge, to protect your privacy and confirm that credit is not granted in your name without your knowledge. You may also submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report, free of charge, or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place.

To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three (3) credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for them as well): (1) full name, with middle initial, and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

Protecting Medical Information.

If you are concerned about protecting your medical information, the following practices can provide additional safeguards to protect against medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.

- Review your “explanation of benefits statement” which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

For Alabama Residents: You may contact the Attorney General’s Office for the State of Alabama, Consumer Protection Division, 501 Washington Avenue, Montgomery, AL 36104, www.alabamaag.gov, 1-800-392-5658.

For California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225. This notification was not delayed as a result of any law enforcement investigation.

For Colorado Residents: You can obtain information from the federal trade commission and the credit reporting agencies about fraud alerts and security freezes.

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For District of Columbia Residents: You can obtain information about steps to take to avoid identity theft from the Federal Trade Commission (contact information above) and The District of Columbia Office of the Attorney General, 400 6th Street NW, Washington, D.C. 20001, consumer.protection@dc.gov, <https://oag.dc.gov/>, (202) 737-3400.

For Illinois Residents: You can obtain information from the credit reporting agencies and the Federal Trade Commission about fraud alerts and security freezes (contact information above). You may contact the Illinois Office of the Attorney General, 100 West Randolph Street, Chicago, IL 60601, https://illinoisattorneygeneral.gov/about/email_ag.jsp, 1-800-964-3013.

For Iowa Residents: You may contact the Iowa Office of the Attorney General, 1305 E. Walnut Street, Des Moines, IA 50319, consumer@ag.iowa.gov; www.iowattorneygeneral.gov, 1-888-777-4590.

For Kansas Residents: You may contact the Kansas Office of the Attorney General, Consumer Protection Division, 120 SW 10th Ave, 2nd Floor, Topeka, KS 66612-1597, <https://ag.ks.gov/>, 1-800-432-2310.

For Kentucky Residents: You may contact the Kentucky Office of the Attorney General, Consumer Protection Division, 1024 Capital Center Drive, Suite 200, Frankfort, Kentucky 40601, www.ag.ky.gov, 1-800-804-7556.

For Maryland Residents: You may obtain information about steps you can take to avoid identity theft from the Federal Trade Commission (contact information above) and the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov, 1-888-743-0023.

For Massachusetts Residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html.

For Minnesota Residents: You may contact the Minnesota Office of the Attorney General, 445 Minnesota Street, Suite 1400, St. Paul, MN 55101, www.ag.state.mn.us, 1-800-657-3787.

For Missouri Residents: You may contact the Missouri Office of the Attorney General, Consumer Protection, 207 W. High St., P.O. Box 899, Jefferson City, MO 65102, www.ago.mo.gov, 1-800-392-8222.

For Nevada Residents: You may contact the Nevada Office of the Attorney General, Bureau of Consumer Protection, 100 N. Carson St, Carson City, NV 89701, www.ag.nv.gov, 1-702-486-3132.

For New Mexico Residents: Consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their 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 consumers’ files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit “prescreened” offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their 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: You may obtain information regarding security breach response and identity theft prevention and protection information from the Federal Trade Commission (contact information above) and the New York Office of the Attorney General, Office of the Attorney General, The Capitol, Albany, NY 12224-0341, <https://ag.ny.gov>, 1-800-771-7755.

For North Carolina Residents: You may obtain information about preventing identity theft from the Federal Trade Commission (contact information above) and the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Main Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7266 or 1-919-716-6400.

For Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392.

For Pennsylvania Residents: You may contact the Pennsylvania Office of the Attorney General, Bureau of Consumer Protection, 15th Floor, Strawberry Square, Harrisburg, PA 17120, www.attorneygeneral.gov, 1-800-441-2555.

For Rhode Island Residents: You may contact the Rhode Island Office of the Attorney General, Consumer Protection Division, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 1-401-274-4400.

For Texas Residents: You may contact the Texas Office of the Attorney General, Office of the Attorney General, PO Box 12548, Austin, TX 78711-2548, www.texasattorneygeneral.gov, 1-800-621-0508.

For Wyoming Residents: This notification was not delayed as a result of any law enforcement investigation.

Reporting of identity theft and obtaining a police report. You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

For Iowa Residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts Residents: You have the right to obtain a police report if you are a victim of identity theft.

For North Carolina Residents: You are advised to report any suspected identity theft to law enforcement or to the North Carolina Attorney General.

For Oregon Residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

<<Variable data 5>>>

Buffalo

Chicago

New York

Raleigh

Washington D.C.

www.octillolaw.com



December 16, 2024

VIA EMAIL

Office of the Attorney General
1125 Washington Street SE
P.O. Box 40100
Olympia, WA 98504-0100

Dear Sir or Madam:

On behalf of Kitsap Mental Health Services (“KMHS”), whose office is located at 5455 Almira Dr. NE, Bremerton, WA 98311, and pursuant to Wash. Rev. Code § 19.255.010 *et seq.*, this letter provides notice of a recent data security incident. By providing this notice, KMHS does not waive any rights or defenses regarding the applicability of Washington law or personal jurisdiction.

KMHS is a not-for-profit organization providing a full range of inpatient, outpatient, and residential behavioral health services for children, adults, and families. On October 17, 2024, during routine monitoring of systems, KMHS detected suspicious activity on its business network. KMHS immediately began an investigation and took steps to contain and remediate the situation, including by changing passwords, deploying tools for increased monitoring, reporting to law enforcement, and engaging data security and privacy experts to assist. Due to the nature of the incident, the investigation is still ongoing into what data pertaining to individuals was affected. Currently, the investigation has found evidence that on September 17, 2024, and between October 8, 2024 and October 19, 2024, an unauthorized actor accessed some KMHS systems. There is currently no evidence of identity theft or fraud in connection with this incident.

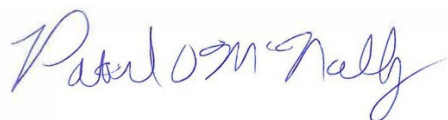
While the investigation is ongoing, KMHS has identified that the following types of information may have been impacted: name, address, birth date, Social Security number, driver’s license or state identification number, medical diagnosis, condition, and/or treatment information, medications, claims information, financial information, and any information on an individual that was created, used, or disclosed in the course of providing health care services.

At this time, KMHS is also providing notice to the Department of Health and Human Services Office for Civil Rights, as well as publishing substitute notice on its website and via media notice, in compliance with the Health Insurance Portability and Accountability Act (“HIPAA”), in order to notify potentially affected individuals while the investigation to identify affected individuals and the specific data elements at risk is ongoing. KMHS will supplement this notice once the investigation is complete.

Please feel free to contact me with any questions at (716) 898-2102 or pmcnally@octillolaw.com.

Sincerely,

OCTILLO

A handwritten signature in blue ink, reading "Patrick D. McNally". The signature is fluid and cursive, with the first name "Patrick" and last name "McNally" clearly legible.

Patrick D. McNally, Esq.
Certified Information Privacy Professional, United States (CIPP/US)

Encl.





Notice of Data Incident

What Happened?

On October 17, 2024, during routine monitoring of our systems, Kitsap Mental Health Services (“KMHS” or “we”) detected suspicious activity in our business network. We immediately began an investigation and took steps to contain and remediate the situation, including by changing passwords, deploying tools for increased monitoring, reporting to law enforcement, and engaging data security and privacy experts to assist.

Due to the nature of the incident, the investigation is still ongoing into what data pertaining to individuals was affected. Currently, the investigation has found evidence that on September 17, 2024 and between October 8, 2024 and October 19, 2024, an unauthorized actor accessed some KMHS systems. There is currently no evidence of identity theft or fraud in connection with this incident.

What Information Was Involved?

Based on the current findings of the investigation, the following types of information may have been impacted: name, address, birth date, Social Security number, driver’s license or state identification number, medical diagnosis, condition, and/or treatment information, medications, claims information, financial information, and any information on an individual that was created, used, or disclosed in the course of providing health care services.

These are general categories of information that we believe may be present within the affected systems and may have been accessed by unauthorized actors during the incident. However, specific individuals and the extent of the information accessed are not yet known. While our investigation is ongoing, we are providing this notice to all individuals who may potentially be affected by this situation.

What We Are Doing

In addition to the actions described above, the KMHS team has been working diligently to continue our investigation and adopt additional safeguards on top of our existing protections. We continue to work with leading data security and privacy firms to aid in our investigation and response, and we are reporting this incident to relevant government agencies.

What Can Impacted Individuals Do?

The investigation is ongoing and the identities of individuals who were affected is not yet known. However, out of an abundance of caution, KMHS encourages individuals to remain vigilant against incidents of identity theft and fraud, to review account statements and explanation of benefits forms, and to monitor free credit reports for suspicious activity and to detect errors. Under U.S. law, individuals are entitled to one (1) free credit report annually from

each of the three (3) major credit reporting bureaus. Additional information and resources are outlined below.

If you have questions for KMHS, you can call us toll-free at 1-800-627-0335, contact us by email at compliance@kmhs.org, or by mail at 5455 Almira Drive NE, Bremerton, WA 98311, Attention: Compliance.

Steps You Can Take to Protect Your Personal Information

To obtain a free credit report, individuals may visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228.

Alternatively, affected individuals can contact the three (3) major credit reporting bureaus directly at the addresses below:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every twelve (12) months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit www.annualcreditreport.com or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Fraud Alert – You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Security Freeze – You may obtain a security freeze on your credit report, free of charge, to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may also submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report, free of charge, or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is

designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place.

To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices – If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General’s office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. Contact information for the Consumer Response Center of the Federal Trade Commission is 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/ or 1-877-IDTHEFT (438-4338).

Protecting Medical Information

If you are concerned about protecting your medical information, the following practices can provide additional safeguards to protect against medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your “explanation of benefits statement” which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.