EXHIBIT 1

This notice may be supplemented if new significant facts are learned subsequent to its submission. By providing this notice, FPS does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about March 3, 2022, FPS learned that certain systems in its computer network had become encrypted with malware deployed by an unknown actor. In response, FPS launched an investigation to determine the full nature and scope of the event. FPS also promptly notified federal law enforcement. The investigation determined that FPS's systems were accessible to the unknown actor between February 28, 2022 and March 3, 2022. Although the investigation was unable to determine whether patient information stored in the impacted systems had actually been viewed or downloaded by the unknown actor, FPS could not rule out the possibility of such activity. Therefore, out of an abundance of caution, a thorough review of the patient information stored within the impacted systems was performed to locate address information for potentially affected individuals in order to provide accurate and complete notices. This review was completed on or around April 25, 2022.

The information that could have been subject to unauthorized access includes name, date of birth, driver's license, and Social Security number.

Notice to Maine Residents

On April 29, 2022, FPS began notifying potentially affected patients by posting notice on its website and issuing notice to prominent media outlets in Arizona and California pursuant to the Health Insurance Portability and Accountability Act (HIPAA). On May 2, 2022, FPS submitted notice to its primary federal regulator, the U.S. Department of Health and Human Services. On or about May 6, 2022, FPS provided written notice of this event to potentially affected patients, including approximately twelve (12) Maine residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, FPS moved quickly to investigate and respond to the event, assess the security of its systems, and identify potentially affected individuals. Further, FPS notified local and federal law enforcement regarding the event. FPS is also working to implement additional safeguards and training to its employees. FPS also established a dedicated toll-free assistance line to address any questions or concerns from notified individuals.

Additionally, FPS is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected events of identity theft or fraud to their credit card company and/or bank. FPS is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for events of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state attorney general, and law enforcement to report attempted or actual identity theft and fraud.

FPS is providing written notice of this event to other appropriate state regulators and to the major consumer reporting agencies.

EXHIBIT A

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

<<Variable Header>>

Dear <<Name 1>>:

FPS Medical Center ("FPS") writes to notify you of a recent event that may affect the security of some of your information. Although there is no indication that your information has been misused in relation to this event, we are providing you with information about the event, our response to it, and what you may do to better protect your personal information, should you feel it appropriate to do so.

What Happened? On or about March 3, 2022, we learned that certain systems in our computer network had become encrypted with malware deployed by an unknown actor. In response, we launched an investigation to determine the full nature and scope of the event. The investigation determined that our systems were accessible to the unknown actor between February 28, 2022 and March 3, 2022. Although the investigation was unable to determine whether patient information stored in the impacted systems had actually been viewed or taken by the unauthorized actor, we could not rule out the possibility of such activity. Therefore, out of an abundance of caution, a thorough review of the patient information stored within the impacted systems was performed to locate address information for potentially affected individuals in order to provide accurate and complete notices. This review was completed by April 25, 2022.

What Information was Involved? The following types of patient information were present in the impacted systems during the event: full name, address, date of birth, driver's license, medical information, including treatment and diagnosis information, and health insurance information. For a limited number of individuals, Social Security number may have also been present. However, we currently have no indication any information has been misused as a result of this event.

What We Are Doing. We take this event and the security of information in our care very 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 are reviewing our existing policies and procedures and implementing additional administrative and technical safeguards to further secure the information in our systems and reduce the risk of recurrence. Further, we reported this event to law enforcement and are notifying appropriate governmental regulators, including the U.S. Department of Health and Human Services.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, explanations of benefits, and monitoring your credit reports for suspicious activity and to detect errors. Please review the enclosed *Steps You Can Take to Help Protect Personal Information* for useful information on what you can do to better protect against possible misuse of your information.

For More Information. If you have additional questions, you may call our dedicated assistance line at 877-587-4021 (toll free), Monday through Friday, 9 am to 9 pm Eastern Time, excluding U.S. holidays. You may also write to FPS at 297 S. Lake Havasu Avenue, Suite 204, Lake Havasu City, AZ 86403.

Sincerely,

Katie Patrick
Practice Manager
FPS Medical Center

Steps You Can Take to Help Protect Personal Information

Monitor 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; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. FPS is located at 297 S. Lake Havasu Avenue, Suite 204, Lake Havasu City, AZ 86403.

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 https://files.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. There are <<RI Count>> known Rhode Island residents impacted by this event.