EXHIBIT 1

By providing this notice, Logan Health 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 November 22, 2021, Logan Health became aware of suspicious activity in its systems including evidence of unauthorized access to one file server that includes shared folders for business operations. With the assistance of third-party forensic experts, Logan Health immediately launched an investigation to determine the nature and scope of the incident and whether any personal information was affected. On January 5, 2022, the investigation determined that there was unauthorized access to certain files, which contained personal information related to patients, employees and business associates.

The information that could have been subject to unauthorized access varies by individual but includes name, Social Security number, and date of birth.

Notice to Maine Residents

On or about February 22, 2022, Logan Health began providing written notice of this incident to all affected individuals, which includes four (4) 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, Logan Health moved quickly to investigate and respond to the incident, assess the security of Logan Health systems, and notify potentially affected individuals. Logan Health is also working to implement additional safeguards and training to its employees. Logan Health is providing access to credit monitoring services for twelve (12) months, through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Logan Health is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Logan Health 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 incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

EXHIBIT A

LOGAN HEALTH

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

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

RE: Notice Data Security Event

Dear <<First_Name>> <<Last_Name>>:

Logan Health Medical Center was recently a victim of a highly sophisticated criminal attack on our information technology systems, which may have involved your personal information. Safeguarding our patients' and employees' personal information is a top priority, and we want you to be aware of what happened and how we have addressed it.

What happened? On November 22, 2021, we discovered suspicious activity including evidence of unauthorized access to one of our eight Logan Health file servers that includes shared folders for business operations. With the assistance of third-party forensic experts we immediately launched an investigation to determine the nature and scope of the incident and whether any personal information was affected. On January 5, 2021, the investigation determined that there was unauthorized access to certain files, which contained protected health information related to employees, including you. There was no unauthorized access to our electronic medical records**.**

What information was involved? Different information may have been involved for each person. The information may have involved your name, Social Security number, address, date of birth, telephone number, or email address.

What are we doing? Although there is no indication that the information was misused, we are offering you 12 months of identity monitoring services at no charge as an extra precaution. Your identity monitoring services, provided by a company called Kroll, include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. In addition, we have deployed additional safeguards to further fortify our information systems.

What you can do: We encourage you to take the steps recommended on the following page to further protect your personal information. You can also activate the complimentary identity monitoring services that we are offering. To enroll in the services, please visit **https://loganhealth.kroll.com**. To receive credit monitoring services, you must be over the age of 18, have established credit in the United States, have a Social Security number in your name, and have a U.S. residential address associated with your credit file. The deadline to enroll in these services is <<b2b_text_6(activation deadline)>>.

For more information: If you have questions or need assistance, please call our designated help line at 1-855-568-2046, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time (excluding major U.S. holidays).

This event is a painful reminder that each of us plays an important role in protecting our patients' private health information. Securing logins and passwords, not clicking on unfamiliar links and being mindful of locations for storing sensitive information are important safeguards that should be followed at all times. Please remember these important tips:

- Never share passwords with anyone, never use someone else's login to access a system, never use the same password also used for personal applications (Facebook, etc.) and never enter your Logan Health login and password into non-Logan Health applications.
- Never open email attachments or click on links within an email unless you know the sender and/or are confident that the communication is legitimate.
- Never download or save ePHI or business confidential data to external drives or portable local storage (including laptop local disk drives and other mobile devices).
- Never transmit ePHI or business confidential data using any data transfer service other than an approved HIT service.

Thank you for all that you do,

Craig Lambrecht, MD
President & CEO
Logan Health

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

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.