EXHIBIT 1

This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, One Brooklyn Health ("OBH") 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 19, 2022, OBH experienced a cybersecurity incident that impacted its computer systems and caused a temporary disruption to its operating procedures. OBH proactively took its systems offline and promptly worked with external specialists to commence an investigation into the nature and scope of the incident. Through its investigation, OBH learned that an unauthorized actor had acquired a limited amount of OBH data during a period of intermittent access to OBH's computer systems between July 9, 2022, and November 19, 2022. OBH, with the assistance of external specialists, then undertook a thorough programmatic and manual review of the contents of the affected data to determine whether they contained any protected health information or otherwise sensitive personal data. This comprehensive and time-consuming review recently concluded on March 21, 2023.

The information that could have been subject to unauthorized access includes name, Social Security number, health insurance information, and medical information.

Notice to Maine Residents

On or about April 20, 2023, OBH began providing written notice of this incident to approximately twenty-four (24) 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 incident, OBH moved quickly to investigate and respond to the incident, assess the security of OBH systems, and work through a thorough and comprehensive process to identify potentially affected individuals. Further, OBH notified city, state, and federal law enforcement authorities regarding the incident. As part of its ongoing commitment to the privacy and security of information in its care, OBH is reviewing its existing policies and training protocols relating to data protection. OBH also implemented enhanced security measures and monitoring tools to mitigate any risk associated with this incident and to better prevent similar incidents in the future. OBH has communicated closely with community stakeholders, insurers, funders, and healthcare authorities regarding this incident.

Additionally, OBH 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. OBH is providing individuals with information on how to place fraud alerts and credit freezes on their credit files, 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.

OBH is providing written notice of this incident to relevant city, state, and federal regulators, as necessary. OBH is also notifying the U.S. Department of Health and Human Services and prominent media pursuant to the Health Insurance Portability and Accountability Act (HIPAA).

EXHIBIT A

One Brooklyn Health
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

April 20, 2023

Dear :

One Brooklyn Health ("OBH") writes to inform you of a recent incident that may affect the privacy of some of your information. OBH provides comprehensive healthcare services to the Central Brooklyn community through its three hospitals, Brookdale Hospital Medical Center, Interfaith Medical Center, and Kingsbrook Jewish Medical Center, nursing homes and health clinics.

This notice provides information about the incident, steps OBH took in response, and resources available to help you better protect your information, should you feel it is appropriate to do so. You are receiving this letter because you have received medical care from OBH.

What Happened? On November 19, 2022, OBH experienced a cybersecurity incident that affected its computer systems and caused a temporary disruption to certain facility operations. OBH proactively took its systems offline and worked with external specialists to commence an investigation into the nature and scope of the incident. Through the investigation, OBH learned that an unauthorized actor acquired a limited amount of OBH data during a period of intermittent unauthorized access to OBH's computer systems between July 9, 2022, and November 19, 2022. A thorough review of the contents of the affected data was subsequently performed to determine whether it contained any sensitive information and to identify affected individuals. On March 21, 2023, OBH concluded the review and determined that your information was in the data that may have been accessed or acquired without authorization.

What Information Was Involved? OBH has no indication that the data affected by this incident has been used to commit identity theft, fraud, or other financial harm to individuals. However, we are notifying you out of an abundance of caution because the information present in the accessed files included your name and:

What We Are Doing. OBH prioritizes its responsibility to safeguard the information it collects in providing services. As such, OBH responded promptly to this incident and has worked diligently to provide you with accurate and complete notice of the incident as soon as possible. In addition, OBH notified law enforcement and regulatory agencies of the incident and continues to cooperate with the authorities' independent investigation efforts. As part of its ongoing commitment to the privacy and security of information in its care, OBH is reviewing its existing policies and training protocols relating to data protection. OBH also implemented enhanced security measures and additional monitoring tools to reduce any risk associated with this incident and to better prevent similar incidents in the future. OBH has communicated with law enforcement and with healthcare authorities regarding this incident.

As an added precaution, OBH is providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or

update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services. Although OBH is covering the cost of these services, due to privacy restrictions, you will need to complete the activation process yourself using the enrollment instructions enclosed.

What You Can Do. In accordance with best practices, as would be recommended in response to any data incident, OBH encourages you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, explanation of benefits, and free credit reports for unexpected activity or errors over the next 12 to 24 months. Any questionable activity detected should be reported to the associated insurance company, health care provider, or financial institution immediately. You can also find out more about how to safeguard your information in the enclosed *Steps You Can Take to Protect Information*. There, you will find additional information about the complimentary credit monitoring services and how to enroll.

For More Information. We understand you may have questions about this incident that are not addressed in this letter. To ensure your questions are answered in a timely manner, please call OBH's dedicated assistance line at: 1-833-570-3025, between 8:00 am and 8:00 pm Monday through Friday Eastern time. You may also reach us directly at: incident@obhny.org. When writing to us, please provide a call back number.

OBH apologizes for any inconvenience this incident may cause you and remains committed to protecting the privacy and security of information in its possession.

Sincerely,

One Brooklyn Health

STEPS YOU CAN TAKE TO PROTECT INFORMATION

Enroll in Complimentary Credit Monitoring Services

To enroll in Credit Monitoring services at no charge, please log on to https://secure.identityforce.com/benefit/obh and follow the instructions provided. When prompted please provide the following unique code to receive services: In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

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 credit 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, 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 a 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	1-800-916-8800
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: 441 4th St. NW #1100 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. One Brooklyn Health is located at 1 Brookdale Plaza, Brooklyn NY 11212.

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; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 56 Rhode Island residents impacted by this incident.