WATSON CLINIC

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

Notice of Data Breach

Dear <<Full Name>>,

Watson Clinic is writing to inform you of an incident involving potential unauthorized access to your information. Earlier this year, we detected a cybersecurity incident involving unauthorized activity in portions of our computer network. We promptly began investigating. Based on the investigation, we determined that the unauthorized third party may have acquired some of your personal information and/or protected health information. We are providing this notice to give you more information on what happened and what we are doing in response.

WHAT HAPPENED
An unauthorized third party gained access to portions of our network starting on January 26, 2024, and we discovered the intrusion on February 6, 2024. We promptly began investigating, engaged third-party cybersecurity experts through outside counsel, and started remediation efforts, including identifying the potentially affected files and engaging a data-review firm to analyze their contents. We received those results in early July 2024 and have been working since that time to compile contact information for notifying impacted individuals.

WHAT INFORMATION WAS INVOLVED
We have not been able to confirm whether the unauthorized third party actually viewed or acquired the files containing your personal information or protected health information. But, because the unauthorized third party potentially accessed those files, we are providing this notice out of an abundance of caution. We determined that the unauthorized third party potentially accessed some of your personal information and protected health information, such as your name, contact information, birthdate, and Social Security number or similar government identifier. The unauthorized third party also potentially accessed some of your medical information, which may include details such as diagnoses, treatments, or medical record numbers.

WHAT WE ARE DOING
Protecting the integrity of the information we maintain is a responsibility we take very seriously. We hired third-party experts to help us address this situation, perform an investigation into the unauthorized activity, and further secure our systems and the information we maintain as we move forward.

WHAT YOU CAN DO
We currently have no evidence that the unauthorized third party has fraudulently used any information involved in this incident. Nonetheless, we encourage you to remain vigilant for any signs of unauthorized financial activity and to review the *Additional Steps You Can Take* guidance included in this letter for steps you can take to protect yourself against fraud. In addition, we are offering a complimentary 2-year membership to Experian's IdentityWorks. You can find instructions for enrolling in that service on the next page.

FOR MORE INFORMATION
Should you have any questions or concerns, you can contact us at 888-244-3078, Monday through Friday, 9:00 a.m. to 9:00 p.m. Eastern Time, and one of our representatives will be happy to assist you. We regret any concern this incident may cause, and thank you for your understanding and patience.

Sincerely,

Robbin Joachim, MSHL, RN, CHC, CHPC
Compliance and Privacy Officer

ADDITIONAL STEPS YOU CAN TAKE

Activate your complimentary credit monitoring – To help protect you from fraud or identity theft, we are offering a complimentary 2-year membership to Experian's IdentityWorks. This product helps detect possible misuse of your personal information. To register, please:

- Ensure that you **enroll by:** <<Enrollment Deadline>> (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
- Provide your **activation code:** <<Activation Code>>
-

If you have questions or want an alternative to enrolling in Experian IdentityWorks online, please contact Experian at (833) 918-1099 by <<Enrollment Deadline>>, and provide them engagement number <<Engagement #>>.

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your account statements and free credit reports. You can also find additional suggestions at www.identitytheft.gov/Info-Lost-or-Stolen.

- You should confirm that your credit card company has the correct address on file for you and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.
- You should obtain and review a free copy of your credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. The alert lasts for one year, but you can renew it.
- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which makes it harder for someone to open an account in your name. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and previous addresses. There is no charge for requesting a security freeze. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission.

Report suspicious activity – If you believe you are the victim of identity theft, consider (1) notifying your Attorney General, local law enforcement, or the Federal Trade Commission; (2) filing a police report and requesting a copy of that report; and (3) visiting IdentityTheft.gov to report the issue and get recovery steps.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting yourself from fraud or identity theft.

Federal Trade Commission	**Equifax**	**Experian**	**TransUnion**
600 Pennsylvania Ave. NW	P.O. Box 740241	P.O. Box 9701	P.O. Box 2000
Washington, DC 20580	Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
(202) 326-2222	(800) 685-1111	(888) 397-3742	(888) 909-8872
www.ftc.gov	www.equifax.com	www.experian.com	www.transunion.com

Maryland Attorney General	**New York Attorney General**	**North Carolina Attorney General**	**Washington, DC Attorney General**
200 St. Paul Place, 25th Floor	The Capitol	9001 Mail Service Center	400 6th St. NW
Baltimore, MD 21202	Albany, NY 1224	Raleigh, NC 27699	Washington, DC 20001
(888) 743-0023	(800) 771-7755	(919) 716-6400	(202) 727-3400
www.marylandattorneygeneral.gov	www.ag.ny.gov	www.ncdoj.gov	www.oag.dc.gov

You can also find your Attorney General's contact information at: https://www.usa.gov/state-attorney-general.

WATSON CLINIC

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

Notice of Data Breach

Dear <<Full Name>>,

Watson Clinic is writing to inform you of an incident involving potential unauthorized access to your information. Earlier this year, we detected a cybersecurity incident involving unauthorized activity in portions of our computer network. We promptly began investigating. Based on the investigation, we determined that the unauthorized third party may have acquired some of your personal information and/or protected health information. We are providing this notice to give you more information on what happened and what we are doing in response.

WHAT HAPPENED
An unauthorized third party gained access to portions of our network starting on January 26, 2024, and we discovered the intrusion on February 6, 2024. We promptly began investigating, engaged third-party cybersecurity experts through outside counsel, and started remediation efforts, including identifying the potentially affected files and engaging a data-review firm to analyze their contents. We received those results in early July 2024 and have been working since that time to compile contact information for notifying impacted individuals.

WHAT INFORMATION WAS INVOLVED
We have not been able to confirm whether the unauthorized third party actually viewed or acquired the files containing your personal information or protected health information. But, because the unauthorized third party potentially accessed those files, we are providing this notice out of an abundance of caution. We determined that the unauthorized third party potentially accessed some of your personal information and protected health information, such as your name, contact information, birthdate, and some of your medical information (which may include details such as diagnoses, treatments, or medical record numbers).

WHAT WE ARE DOING
Protecting the integrity of the information we maintain is a responsibility we take very seriously. We hired third-party experts to help us address this situation, perform an investigation into the unauthorized activity, and further secure our systems and the information we maintain as we move forward.

WHAT YOU CAN DO
We currently have no evidence that the unauthorized third party has fraudulently used any information involved in this incident. Nonetheless, we encourage you to remain vigilant for any signs of unauthorized financial activity and to review the *Additional Steps You Can Take* guidance included in this letter for steps you can take to protect yourself against fraud.

FOR MORE INFORMATION
Should you have any questions or concerns, you can contact us at 888-244-3078, Monday through Friday, 9:00 a.m. to 9:00 p.m. Eastern Time, and one of our representatives will be happy to assist you. We regret any concern this incident may cause, and thank you for your understanding and patience.

Sincerely,

Robbin Joachim, MSHL, RN, CHC, CHPC
Compliance and Privacy Officer

ADDITIONAL STEPS YOU CAN TAKE

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your account statements and free credit reports. You can also find additional suggestions at www.identitytheft.gov/Info-Lost-or-Stolen.

- You should confirm that your credit card company has the correct address on file for you and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.
- You should obtain and review a free copy of your credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. The alert lasts for one year, but you can renew it.
- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which makes it harder for someone to open an account in your name. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and previous addresses. There is no charge for requesting a security freeze. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission.

Report suspicious activity – If you believe you are the victim of identity theft, consider (1) notifying your Attorney General, local law enforcement, or the Federal Trade Commission; (2) filing a police report and requesting a copy of that report; and (3) visiting IdentityTheft.gov to report the issue and get recovery steps.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting yourself from fraud or identity theft.

Federal Trade Commission	**Equifax**	**Experian**	**TransUnion**
600 Pennsylvania Ave. NW	P.O. Box 740241	P.O. Box 9701	P.O. Box 2000
Washington, DC 20580	Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
(202) 326-2222	(800) 685-1111	(888) 397-3742	(888) 909-8872
www.ftc.gov	www.equifax.com	www.experian.com	www.transunion.com

Maryland Attorney General	**New York Attorney General**	**North Carolina Attorney General**	**Washington, DC Attorney General**
200 St. Paul Place, 25th Floor	The Capitol	9001 Mail Service Center	400 6th St. NW
Baltimore, MD 21202	Albany, NY 1224	Raleigh, NC 27699	Washington, DC 20001
(888) 743-0023	(800) 771-7755	(919) 716-6400	(202) 727-3400
www.marylandattorneygeneral.gov	www.ag.ny.gov	www.ncdoj.gov	www.oag.dc.gov

You can also find your Attorney General's contact information at: https://www.usa.gov/state-attorney-general.