SQUIRE PATTON BOGGS

Squire Patton Boggs (US) LLP
1000 Key Tower
127 Public Square
Cleveland, OH 44114

O +1 216 479 8500
F +1 216 479 8780
squirepattonboggs.com

Colin R. Jennings
T +1 216 479 8420
colin.@squirepb.com

August 30, 2022

VIA OVERNIGHT DELIVERY AND EMAIL DELIVERY TO:
IDTHEFT@OAG.STATE.MD.US

Office of the Attorney General
200 St. Paul Place
Baltimore, Maryland 21202

Attention: Security Breach Notification

Re: Notice of a Cybersecurity Event by New Jersey Department of Health

To Whom It May Concern,

This letter shall serve as notice to the Office of the Maryland Attorney General on behalf of our client, New Jersey Department of Health ("NJ DOH") of a network security incident ("Incident") that may have involved personally identifiable information ("PII") of Maryland residents.

On June 30, 2022, Trenton Psychiatric Hospital ("TPH" or the "hospital") within the Division of Behavioral Health Services of the NJ DOH, received notification of an alleged cyber security incident experienced by Clairsol Inc. ("Clairsol"). Clairsol is a third party vendor that provides medical translation and dictation services to New Jersey's State psychiatric hospitals, including TPH. The investigation to date indicates that an unauthorized individual gained access to and obtained limited protected health records of certain current and former patients of TPH.

The confidentiality of TPH's patients' information is one of TPH's top priorities. Immediately upon learning of the Incident, TPH took steps to contain the Incident and conduct a thorough investigation. In particular, the IT team that supports the hospital immediately notified New Jersey State police as well as the New Jersey Cybersecurity & Communications Integration Cell to assist with investigating this Incident. The IT team also promptly blocked all access to Clairsol's system and requested Clairsol to disable access and take Clairsol's system offline, which

on July 1, 2022 Clairsol confirmed it took the requested action. Prior to resuming the use of Clairsol's systems, as appropriate, the IT team that supports the hospitals will conduct a thorough investigation and assessment to identify and implement additional remedial measures, as appropriate.

On or about August 9, 2022, TPH determined the Incident may have included limited Maryland residents. While NJ DOH's investigation is still ongoing, there is no evidence that any PII of any Maryland resident was misused. In an abundance of caution, however, and because NJ DOH is committed to protecting Maryland's residents' PII, NJ DOH has proactively notified all individuals whose PII could have been compromised.

The types of PII that may have been impacted for affected Maryland individuals includes health information, specifically:

- Name
- Patient Identification Number
- Facility Name
- Internal Identification Number

The number of affected individuals from Maryland is approximately two (2) and, to date, the total number of affected individuals for this Incident is approximately 850. As provided in the enclosed template notification letter, NJ DOH will provide these individuals with twelve (12) months of credit monitoring and identity theft insurance free of charge. We will inform you as we learn additional pertinent information about the Incident, as appropriate. Any questions about this Incident can be directed to me at colin.jennings@squirepb.com.

Sincerely,

Squire Patton Boggs (US) LLP

Colin Jennings
cc: Ericka Johnson, Esq.
Attached: NJDOH – TPH Individual Notice

New Jersey Department of Health
C/O Cyberscout
P.O. Box 3923
Syracuse, NY 13220

State of New Jersey
DEPARTMENT OF HEALTH
DIVISION OF BEHAVIORAL HEALTH SERVICES
TRENTON PSYCHIATRIC HOSPITAL

First and Last Name
Address Line 1
Address Line 2

August 17, 2022

Dear First Name:

We are writing to share with you important information regarding a network security incident ("Incident") that involved your protected health information ("PHI"). We take this Incident very seriously and are providing you with information, as well as access to resources, so that you can better protect your PHI.

What Happened:

On June 30, 2022, Trenton Psychiatric Hospital ("TPH" or the "hospital") within the Division of Behavioral Health Services of the New Jersey Department of Health, received notification of an alleged cyber security-incident experienced by Clairsol Inc. ("Clairsol"). Clairsol is a third party vendor that provides medical translation and dictation services to New Jersey's State psychiatric hospitals, including TPH. The investigation to date indicates that an unauthorized individual gained access to and obtained limited protected health records of certain current and former patients of TPH.

Immediately upon becoming aware of the Incident, all hospital access to Clairsol's system was blocked and a request was made to Clairsol to disable access and take Clairsol's system offline. An investigation was immediately launched to investigate, address, and resolve the Incident and Clairsol was directed to do the same.

While our investigation is still ongoing, there is no evidence that your PHI was misused. **Because we are committed to protecting your personal data, we are proactively providing you this notice, in an abundance of caution, so that you may diligently monitor your information.**

What Information was Involved:

Your name, patient identification number, facility name, and internal identification number.

What TPH is Doing:

The confidentiality of our patients' PHI is one of TPH's top priorities. Immediately upon learning of the Incident, we took steps to contain the Incident and conduct a thorough investigation. In particular, the IT team that supports the hospital immediately notified New Jersey State police as well as the New Jersey Cybersecurity & Communications Integration Cell to assist with investigating this Incident. The IT team also promptly blocked all access to Clairsol's system and requested Clairsol to disable access and take Clairsol's system offline. Prior to resuming the use of Clairsol's systems, as appropriate, the IT team will conduct a thorough investigation and assessment to identify and implement additional remedial measures. As such, we have already strengthened our system, and will continue to do so throughout this response process and beyond.

Credit Monitoring Services:

While TPH is not aware of any identity fraud or improper use of any PHI as a direct result of this Incident, we have arranged to have Cyberscout provide you with twelve (12) months of complimentary credit monitoring services through Identity Force and identity theft insurance. To activate your membership in these services, please follow the steps outlined at the end of this letter.

As a best practice, we recommend that you remain vigilant in regularly reviewing and monitoring your account statements and Explanation of Benefits for any discrepancies or appearance of fraudulent activity to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on your accounts, please contact your financial institution or health insurance carrier. We have provided additional information below about steps you can take to protect yourself against fraud and identity theft.

What You Can Do:

Please note, you are not required to do anything.

The internet and technology is a part of our daily lives. Below, are some best practices and recommendations outlined by the State of New Jersey's Cybersecurity Communications & Integration Cell ("NJCCIC"), which is New Jersey's central location for learning and sharing about cybersecurity and is operated by the New Jersey Office of Homeland Security and Preparedness.

Those guidelines are as follows:

- Ensure your devices, such as computers and cell phones have enabled privacy safeguards.
- Only use secured and trusted networks when using the internet for sensitive things, such as shopping and banking.
- Do not share your account credentials with anyone or save them on your computer.
- When establishing passwords on accounts, use a combination of: upper/lower case letters, numbers and symbols.
- It is recommended to change your passwords every 90 days.
- If you come across unusual activity on your banking or shopping accounts, report it directly to the account facilitators.

Note, any person can become a member of the NJCCIC and can receive best practice tips to their email by joining at https://www.cyber.nj.gov/members/. Additional resources regarding daily cybersecurity tips can also be found on the NJCCIC's website located at https://www.cyber.nj.gov/learn/cybersecurity-best-practices/.

For More Information:

If you have any questions about this notice or the Incident, please telephone the Cyberscout call center at 1-800-405-6108 from 8:00 am to 8:00 pm ET, Monday through Friday, excluding holidays, for ninety (90) days from the date of this letter.

We value you and sincerely apologize for any inconvenience caused by this Incident. Thank you for your understanding.

Sincerely,

Neela Sookdeo

Neela Sookdeo
HIPAA Privacy Officer

Credit Monitoring Services

In response to the Incident, TPH has engaged Cyberscout to provide the following services through Identity Force:

- Single Bureau Credit Monitoring, Report and Score*
- Cyber Monitoring
- Identity Protection Services
- Identity Resolution Services
- $1,000,000 in Identity Theft Insurance

These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. A notification will be sent to you the same day that the changes or updates takes place with the bureau. Cyber monitoring will look out for your personal data on the dark web and alert you if your personally identifiable information is found online. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event you become a victim of identity theft, as well as a $1,000,000 insurance reimbursement policy. To safeguard your privacy and security, you will be asked to verify your identity before monitoring can be activated.

Representatives are available for ninety (90) days from the date of this letter, to assist you with questions regarding this Incident, between the hours of 8:00 am to 8:00 pm ET, Monday through Friday, excluding holidays. Please call the help line 1-800-405-6108 and supply the fraud specialist with your unique code listed below. To extend these services, enrollment in the monitoring services described above is required.

How do I enroll for the free services?

To register your account and activate your services type the following URL into your browser: **https://secure.identityforce.com/benefit/njdeptofhealth** and follow the instructions provided. When prompted please provide the following unique code to receive services: **<Unique Code>**

Important – you must register your account and activate your monitoring services within 90 days from the date of this letter, otherwise your ability to access the services will expire.

* Services marked with an "*" require 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.

Additional Information

To protect against possible fraud, identity theft or financial loss, we encourage you to remain vigilant, review your account statements, and monitor your credit reports. Provided below are the names and contact information for the three major U.S. credit reporting agencies and additional information about steps you can take to obtain a free credit report and to place a fraud alert, credit freeze, or credit lock on your credit report. If you believe you are a victim of fraud or identity theft, you should consider contacting your local law enforcement agency, your State's Attorney General, or the Federal Trade Commission.

INFORMATION ON OBTAINING A FREE CREDIT REPORT

U.S. residents are entitled under U.S. law to one (1) free credit report annually from each of the three (3) major credit reporting agencies. To order a free credit report, visit www.annualcreditreport.com or call toll-free (877) 322-8228.

INFORMATION ON IMPLEMENTING A FRAUD ALERT, CREDIT FREEZE, OR CREDIT LOCK

To place a fraud alert, credit freeze, or credit lock on your credit report, you must contact the three (3) credit reporting agencies below:

Equifax:	Experian:	TransUnion:
Consumer Fraud Div.	Credit Fraud Center	TransUnion LLC
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022-2000
1-888-766-0008	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Fraud Alert: Consider contacting one of the three (3) major credit reporting agencies at the addresses above to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might protect against someone else obtaining credit in your name.

To place a fraud alert, contact any of the three (3) major credit reporting agencies listed above and request that a fraud alert be put on your file. The agency that you contacted must notify the other two agencies. A fraud alert is free and lasts ninety (90) days, but can be renewed.

Credit Freeze: A credit freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report until the freeze is lifted. There is no cost to place a credit freeze. When a credit freeze is in place, no one— including you—can open a new account. As a result, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services.

To place a credit freeze, contact all three credit reporting agencies listed above and provide the personal information required by each agency to place a freeze, which may include:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;

4. If you have moved in the past five (5) years, the addresses where you have lived over the prior 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. If you are a victim of identity theft, a copy of either a police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

When you place a credit freeze, you will be provided a PIN to lift temporarily or remove the credit freeze. A credit freeze generally lasts until you lift or remove it, although in some jurisdictions it will expire after seven (7) years.

Credit Lock: Like a credit freeze, a credit lock restricts access to your credit report and prevents anyone from opening an account until unlocked. Unlike credit freezes, your credit can typically be unlocked online without delay. To lock your credit, contact all three (3) credit reporting agencies listed above and complete a credit lock agreement. The cost of a credit lock varies by agency, which typically charges monthly fees.

ADDITIONAL RESOURCES

You may also contact the U.S. Federal Trade Commission ("FTC") for further information on fraud alerts, credit freezes, credit locks, and how to protect yourself from identity theft. The FTC can be contacted at 400 7th St. SW, Washington, DC 20024; telephone 1-877-382-4357; or www.consumer.gov/idtheft.

Certain states require that we provide contact information for state Attorneys General. If you currently reside in one of the states below, your state Attorney General may also have advice on preventing identity theft and you should report instances of known or suspected identity theft to law enforcement, your State Attorney General, and/or the FTC.

Maryland Residents: The Attorney General can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, MD 21202; (888) 743-0023; or http://www.oag.state.md.us.

North Carolina Residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; (919) 716-6400; or http://www.ncdoj.gov.

Iowa Residents: The Attorney General can be contacted at 1305 E. Walnut St. Des Moines, IA 50319; (515) 281-5164; or https://www.iowaattorneygeneral.gov/.

Oregon Residents: The Attorney General can be contacted at 1162 Court St. NE Salem, OR 97301-4096; (877) 877-9392; or https://www.doj.state.or.us/.

Rhode Island Residents: The Attorney General can be contacted at 4 Howard Avenue Cranston, RI 02920; (401) 274-4400; or http://www.riag.ri.gov/index.php. You may also file or obtain any police report filed in regard to this incident.

District of Columbia Residents: The Attorney General can be contacted at Office of Attorney General, 400 6th Street, NW, Washington, DC 20001; (202) 727-3400; or https://oag.dc.gov/.