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

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

Notice of Data Breach

Dear <<First_Name>> <<Last_Name>>,

Hopscotch Primary Care ("Hopscotch") is writing to notify you of a recent incident that may affect the privacy of your protected health information (PHI) created or received while you were a patient of Cannon Family Health, which now operates as "Hopscotch Primary Care." We wish to provide you with information about the incident, our response, and steps you can take to protect against misuse of your information.

What Happened? On August 27, 2024, Hopscotch learned of a physically isolated incident involving a limited set of legacy Cannon Family Health physical paper records that were accessed by a bad actor, who had no affiliation with Hopscotch. Upon learning of the matter, Hopscotch immediately began cooperating with the Buncombe County Sheriff's Office to investigate and remediate the incident.

Thanks to the prompt work of local law enforcement, the bad actor was detained and faces prosecution. Our ability to investigate this matter has been impacted by difficulties presented both by the law enforcement nature of this incident and the devastating effects of Hurricane Helene, but we continue to investigate. We can also assure you that while some of Cannon Family Health's legacy paper files were impacted by this incident, Hopscotch maintains a separate comprehensive and secure electronic file system housing current medical records which were not affected.

What Information Was Involved? On September 19, 2024, law enforcement gave Hopscotch access to a portion of the legacy paper records involved so we could begin assessing any potential impact. The investigation to date has determined that some of your PHI may have been present in the legacy files that were compromised by the bad actor. At this time, we believe the information was limited to information contained on billing statements that included your name, the amount paid, and the fact that you were a Cannon Family Health patient. These billing statements did not include clinical information and did not include financial account information such as bank account or credit card numbers. We are continuing to investigate this incident, and we will contact you again if we find that any of your additional PHI may have been compromised.

What We Are Doing. We take this incident and the security of information in our care seriously. Upon learning of this incident, we worked with law enforcement to determine the nature and scope of the compromise. We are continuing to work with law enforcement to understand the scope of the incident and the extent to which information was compromised. We are also working to implement policies and procedures to provide further protection for patient records but, as noted, Hopscotch maintains a separate electronic medical record system for current treatment records and that system was not impacted by this incident.

What You Can Do: Please review the information contained in the attached *Steps You Can Take to Help Protect Your Information*. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, monitoring free credit reports you are entitled to receive, and immediately reporting any suspicious activity or incidents of suspected identity theft or fraud to your bank or other financial institution(s).

If you have questions, please call (866) 651-8551, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Standard Time, excluding major U.S. holidays. You may also write to Hopscotch Primary Care, 6 Brooklet Street, Asheville, NC 28801.

Sincerely,

David Thurlow

David Thurlow
Chief Operating Officer

Steps You Can Take To Help Protect Personal Information

Monitor Your Accounts

Under U.S. law, each consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus: Equifax, Experian, and TransUnion. We recommend that you periodically obtain a credit report from each nationwide credit reporting agency and request deletion of any information relating to fraudulent transactions. To order a 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 credit report.

You have the right to place an initial or extended "fraud alert" on your credit file at no cost. An initial fraud alert is a 1year alert that is placed on a credit file. If a fraud alert is displayed on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. Victims of identity theft are entitled to an extended fraud alert, which is a 7-year fraud alert. If you wish to place a fraud alert, contact any of the three major credit reporting bureaus.

You also have the right to place a free "credit freeze" on your credit report pursuant to 15 U.S.C. § 1681c-1, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your express consent. However, using a credit freeze to control access to the personal and financial information in a credit report may delay, interfere with, or prohibit the timely approval of any request or application made 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. To request a credit freeze, you may need to provide some or all of the following information, depending on whether the request is made online, by phone, or by mail:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number or copy of Social Security card;
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. If you're a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency.

Should you wish to place a credit freeze or fraud alert, contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
www.equifax.com/personal/credit-report-services/ 1-888-298-0045 Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069 Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	www.experian.com/help/ 1-888-397-3742 Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013 Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	www.transunion.com/credit-help 1-800-916-8800 TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016 TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

In addition to the options outlined above, you may place an alert with ChexSystems. Chex Systems, Inc. is a consumer reporting agency governed by the Fair Credit Reporting Act and other laws. ChexSystems provides account verification services to its financial institution members to aid them in identifying account applicants who may have a history of account mishandling (for example, people whose accounts were overdrawn and then closed by them or their bank). In short, ChexSystems is like the credit reporting agencies (Equifax, Experian, TransUnion) but specific to checking/savings history instead of credit/loan history. ChexSystems offers two protections:

- **Consumer Report Security Alert.** This puts a flag on your consumer file notifying banking institutions that they must take additional steps to confirm the identity of the person initiating the action (much like placing a fraud alert with the credit reporting agencies). You may request a 90-day alert, which is the default, though you may extend it to 7 years if you complete the ChexSystems ID Theft affidavit form (available online), have the affidavit notarized, and send the notarized affidavit to ChexSystems. To set the Consumer Report Security Alert, call (888) 478-6536 or online by visiting www.chexsystems.com.

- **Consumer Report Security Freeze.** This will prohibit ChexSystems from releasing any information in your consumer file without your express authorization, meaning you have to contact ChexSystems and lift the freeze in order for your information to be released (much like placing a freeze with the credit reporting agencies). You should be aware that taking advantage of this right may delay or prevent timely approval from any user of your consumer report that you wish to do business with. The third party will receive a message indicating that you have blocked your information. To set the Consumer Report Security Freeze, call (800) 887-7652 or online by visiting www.chexsystems.com.

Additional Information

You can obtain information from the Federal Trade Commission ("FTC"), credit reporting bureaus listed above, and your state Attorney General regarding identity theft, fraud alerts, and credit freezes, and steps you can take to protect personal information. The FTC may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 877-ID-THEFT (877-438-4338); and TTY: 866-653-4261. The FTC also encourages those who discover that their information has been misused to file a complaint using the FTC's contact information above. You also have the right to file and obtain a copy of your police report if you experience identity theft or fraud. Note that in order to file an identity theft report with law enforcement, you will likely need to provide some proof that you have been a victim. You should also report instances of known/suspected identity theft to local law enforcement and your state Attorney General.

For District of Columbia residents, you may obtain information about steps to avoid identity theft from the FTC and the Office of the Attorney General for the District of Columbia. Contact: 400 6th Street, 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 https://www.marylandattorneygeneral.gov/.

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, you may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and ncdoj.gov.

For Oregon Residents, the Oregon Division of Financial Regulation (DFR) oversees residential mortgage loan servicers who are responsible for servicing residential mortgage loans in connection with real property located in Oregon and persons required to have a license to service residential mortgage loans in this state. If you have questions regarding your residential mortgage loan, contact your servicer at 866-882-8187 or www.planethomelending.com. To file a complaint about unlawful conduct by an Oregon licensee or a person required to have an Oregon license, call DFR at 888-877-4894 or visit dfr.oregon.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; riag.ri.gov; and 401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event.