National Church Residences
BATH ROAD

SUBSTITUTE NOTICE
July 1, 2020

We recently learned of a data incident involving one of our third party vendors, Access Companies ("Access"). Access helps us process insurance claims.

Access discovered that an unidentified individual accessed an employee's email account last year. A computer security firm conducted an investigation of Access's computer systems, networks and the affected email account. Based on this investigation, it is our understanding that this incident was limited to the affected email account and did not impact Access's computer systems or network. Additionally, the investigators did not find any evidence that the unidentified individual accessed any particular information or viewed or acquired any specific emails or attachments stored within the affected email account during this incident.

Nevertheless, out of an abundance of caution, emails stored in the affected email account were reviewed to determine whether any of the emails contained personal information. Access determined that some of the emails in that account may have contained certain personal information related to a small number of patients. These personal identifiers may have included name, address, date of birth, medical record number, date of service, provider name, and/or insurance information. To date, we are unaware of any fraud or misuse of anyone's information as a result of this incident.

We are in the process of notifying individuals whose personal information was stored in the affected email account. We apologize for any inconvenience this incident may have caused. If you have any questions or concerns, please feel free to contact Access's Provider Services Director, Casey Beard, at 614-345-5001 (ext. 212), or (877-708-2223), or by email at caseyb@accesselite.com.

Individuals who have concerns about the misuse of their information can take the following steps to protect themselves:

Filing a Police Report for Suspicious Activity

We encourage you to remain vigilant of identity theft or fraud. You should review account statements, explanation of benefits, and credit reports and report any suspicious activity or suspected identity theft. You have the right to file a police report if you experience identity theft or fraud. If you do find suspicious activity of identity theft or fraud, call your local police or sheriff's office and file a police report of identity theft. Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records. In addition, you should report identity theft to your state's Attorney General and to the Federal Trade Commission ("FTC"). This notice has not been delayed by law enforcement.

Monitoring Your Accounts

You may obtain a free copy of your credit report from each of the credit bureaus once a year by visiting http://www.annualcreditreport.com, or calling 877-322-8228. Hearing impaired consumers can access TDD service at 877-730-4104. You may contact the nationwide credit bureaus at:

Equifax, 866-349-5191, P.O. Box 740241, Atlanta, GA 30374, www.equifax.com/FCRA.
Experian, 888-397-3742, P.O. Box 9701, Allen, TX 75013, www.experian.com.
TransUnion, 800-916-8800, P.O. Box 2000, Chester, PA 19022, www.transunion.com.

You may also place a fraud alert or security freeze on your credit report at no cost. A fraud alert is a notice that can be

placed on a consumer's credit report that alerts companies who may extend credit that the consumer may have been a victim of identity theft or fraud. When 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. There are two types of fraud alerts: an "initial" fraud alert that lasts for one year, and an "extended" fraud alert for victims of identity theft or fraud that lasts seven years. A fraud alert should not affect your ability to get a loan or credit, but it may cause some delay if you are applying for credit. To place a fraud alert, please contact one of the credit reporting agencies at:

Equifax, 888-836-6351, P.O. Box 105069, Atlanta, GA 30348, www.equifax.com/personal/credit-report-services
Experian, 888-397-3742, P.O. Box 9554, Allen, TX 75013, www.experian.com/fraud/center.html
TransUnion, 800-680-7289, P.O. Box 2000, Chester, PA 19016, www.transunion.com/fraud-alerts.

Alternatively, you may place a security freeze on your file. Security freezes will prevent new credit from being opened in your name without the use of a personal identification number or password that will be issued by the credit reporting agencies after you initiate the freeze. In order to place a security freeze, you may be required to provide the credit reporting agencies with information that identifies you. A security freeze can make it more difficult for someone to get credit in your name, but it also may delay your ability to obtain credit. The credit reporting agencies may not charge a fee to place a freeze or remove a freeze. To place a security freeze, please contact one of the agencies at:

Equifax, 888-298-0045, P.O. Box 105788, Atlanta, GA 30348, www.equifax.com/personal/credit-report-services
Experian, 888-397-3742, P.O. Box 9554, Allen, TX 75013, www.experian.com/freeze/center.html
TransUnion, 888-909-8872, P.O. Box 160, Woodlyn, PA 19094, www.transunion.com/credit-freeze.

Additional Information

You may find additional information about fraud alerts, security freezes, and suggestions you can take to protect yourself from identity theft or fraud by contacting the FTC or your state Attorney General.

The FTC provides suggestions for actions you may take in the event of identity theft at www.consumer.ftc.gov/features/feature-0014-identity-theft. You may also call the FTC for more information at 1-877-ID-THEFT (438-4338) (TTY: 1-866-653-4261), or write Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You may also review helpful websites to learn more about consumer protection measures related to this type of fraud, i.e. AHIMA's *Medical Identity Theft Response Checklist for Consumers,* which can be found at http://bot.ly/2pHDcqV.

- Closely monitor your account statements, explanation of benefits, and credit reports closely.
- You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- As an alternative to a security freeze, 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 1-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.
- Do not provide personal information to anyone requesting information from you by telephone or e-mail. Be wary of scams that may appear to offer protection but are really trying to get personal information from you. If you have any suspicions about the authenticity of an email or text, do not click the links in it.
- If you believe any personal information has been compromised, notify local law enforcement to assist you.
- Review helpful websites to learn more about consumer protection measures related to this type of fraud, i.e. AHIMA's *Medical Identity Theft Response Checklist for Consumers,* which ca be found at http://bot.ly/2pHDcqV.