EXHIBIT A

BOYS TOWN
National Research Hospital

Processing Center ● P.O. BOX 141578 ● Austin, TX 78714

00001
ACD1234

00001
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

July 20, 2018

Re: Notice of Data Breach

Dear John Sample:

Boys Town National Research Hospital ("Boys Town") is writing to notify you of an incident that may affect the security of some of your personal information. We take this incident very seriously. This letter provides details of the incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it is appropriate to do so.

What Happened? On May 23, 2018, Boys Town became aware of unusual activity relating to an employee email account. We quickly launched an investigation to determine what may have happened and what information may have been affected, working together with computer forensics experts. Our investigation determined that an unknown individual had access to the email account on May 23, 2018. We reviewed the email account to identify what personal information was stored within the email account. Although we are unaware of any actual or attempted misuse of your personal information, we are providing you this notification out of an abundance of caution because your information was present in the account on May 23, 2018.

What Information Was Involved? Our investigation confirmed the information present in the impacted email account includes your name and ( ).

What Are We Doing. Information privacy and security are among our highest priorities. Boys Town has strict security measures in place to protect information in our care. Upon learning of this incident, we quickly took steps to confirm the security of our systems, including our employee email accounts. We reset passwords for Boys Town email accounts, implemented increased security measures for email account access, conducted additional employee training, and reviewed our company policies and procedures relating to data security. We also notified necessary regulatory and law enforcement bodies. In an abundance of caution, we are also notifying potentially affected individuals, including you, so that you may take further steps to best protect your personal information, should you feel it is appropriate to do so. Although we are not aware of any actual or attempted misuse of information as a result of this event, we arranged to have AllClear ID protect your identity for 12 months at no cost to you as an added precaution.

What Can You Do. You may review the information contained in the attached "Steps You Can Take to Protect Your Information." You may also enroll to receive the identity protection services we are making available to you. Boys Town will cover the cost of this service; however, you will need to enroll yourself in this service.

For More Information. We recognize that you may have questions not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-855-686-9425 (toll free), Monday through Saturday, 8:00 a.m. to 8:00 p.m., CT.

We sincerely regret any inconvenience this incident may cause you. Boys Town remains committed to safeguarding information in our care and we will continue to take proactive steps to enhance the security of our systems.

Sincerely,

Nisha Nair, J.D.
Boys Town National Research Hospital Privacy Officer

Steps You Can Take to Protect Your Information

Enroll in Credit Monitoring

As an added precaution, we have arranged to have AllClear ID protect your identity for 12 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-686-9425 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Fraud Alerts with Credit Monitoring: This service offers the ability to set, renew, and remove 90-day fraud alerts on your credit file to help protect you from credit fraud. In addition, it provides credit monitoring services, a once annual credit score and credit report, and a $1 million identity theft insurance policy. To enroll in this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-686-9425 using the following redemption code: Redemption Code.

Please note: Following enrollment, additional steps are required by you in order to activate your phone alerts and fraud alerts, and to pull your credit score and credit file. Additional steps may also be required in order to activate your monitoring options.

Monitor Your Accounts. You may take action to protect against possible identity theft or financial loss, should you feel it is appropriate to do so. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your bank account statements, credit or debit card statements, and health insurance policy statements, and to monitor your credit reports and explanation of benefits forms for suspicious activity.

Credit Reports. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

Fraud Alerts. At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax Consumer Fraud Division	Experian	TransUnion
P.O. Box 740256	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
1-888-766-0008	1-888-397-3742	1-800-680-7289
www.alerts.equifax.com	www.experian.com	www.transunion.com

Security Freeze. You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised 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. If you have been a victim of identity theft, and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee (typically $5 to $15 each) to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files.

To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	Experian Security Freeze	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-685-1111	1-888-397-3742	1-888-909-8872
https://www.freeze.equifax.com	www.experian.com/freeze/center.html	www.transunion.com/securityfreeze

Additional Information. You can further educate yourself regarding identity theft, and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580; www.ftc.gov/idtheft; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC. You can also further educate yourself about placing a fraud alert or security freeze on your credit file by contacting the FTC or your state's Attorney General. This notice has not been delayed as a result of a law enforcement investigation.

For Maryland residents, the Maryland Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. Boys Town is located at: 14100 Crawford Street, Boys Town, NE 68010.

For North Carolina residents, the North Carolina Attorney General can be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General can be contacted by mail at 150 South Main Street, Providence, RI 02903; by phone at (401) 274-4400; and online at www.riag.ri.gov. You have the right to file and obtain a police report if you ever experience identity theft or fraud. A total of four (4) Rhode Island residents were impacted by this incident.

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 agencies 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 violators. 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. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should also be reported to law enforcement.

EXHIBIT B

Notice of Data Incident

Notice of Data Security Incident:
Boys Town National Research Hospital ("Boys Town") - July 20, 2018

What Happened? On May 23, 2018, Boys Town became aware of unusual activity relating to an employee email account. We quickly launched an investigation to determine what may have happened and what information may have been affected, working together with computer forensics experts. Our investigation determined that an unknown individual had access to the email account on May 23, 2018. We reviewed the email account to identify what personal information was stored within the email account. On or around July 3, 2018, Boys Town confirmed the personal information that may have been accessible as a result of the incident and the identities of the individuals relating to this personal information.

What Information Was Involved? The investigation in this matter confirmed that the following types of personal information related to Boys Town patients and employees may have been accessible as a result of the incident: name, date of birth, Social Security number, diagnosis or treatment information, Medicare or Medicaid identification number, medical record number, billing/claims information, health insurance information, disability code, birth or marriage certificate information, Employer Identification Number, driver's license number, passport information, banking or financial account number, and username and password. To date, Boys Town has not received any reports of the misuse of this information.

What is Boys Town Doing? Boys Town takes this incident and the security of personal information seriously. Upon learning of this incident, Boys Town moved quickly to confirm whether personal information may have been affected by this incident, to identify the individuals related to this personal information, to put in place resources to assist them, and to provide them with notice of this incident. Boys Town is reviewing its existing policies and procedures, and implementing additional safeguards to further protect information stored in our systems. Boys Town reported this incident to law enforcement and is notifying state and federal regulators, as required. We are also notifying potentially affected individuals and will be offering these individuals access to 12 months of free identity protection services.

What You Can Do? Boys Town established a dedicated hotline for potentially affected individuals to contact with questions or concerns regarding this incident. For additional information, please call 1-855-686-9425 (toll-free), Monday through Saturday from 8:00 a.m. to 8:00 p.m. CT. Potentially affected individuals may also consider the information and resources outlined below.

Monitor Your Accounts.
Boys Town encourages potentially impacted individuals to remain vigilant against incidents of identity theft and fraud by reviewing their accounts, explanations of benefits, and credit reports for suspicious activity, and to report any suspicious activity to the affiliated institutions immediately.

Credit Reports. Under U.S. law, individuals with credit reports are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

Fraud Alerts. At no charge, individuals with credit files may also have these credit bureaus place a "fraud alert" on their file that alerts creditors to take additional steps to verify the individual's identity prior to granting credit in that person's name. Note, however, that because it tells creditors to follow certain procedures to protect the individual, if you take this step it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms a fraud alert, the others are notified to place fraud alerts on that person's file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below:

Equifax Consumer Fraud Division
P.O. Box 740256
Atlanta, GA 30374
1-888-766-0008
www.alerts.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19106
1-800-680-7289
www.transunion.com

Security Freeze. Individual's with credit files may also place a security freeze on their credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised 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. If you have been a victim of identity theft and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. Fees vary based on where you live, but commonly range from $0 to $15 each ($5 each in Massachusetts). You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111
https://www.freeze.equifax.com

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
www.transunion.com/securityfreeze

Additional Information. You can further educate yourself regarding identity theft, and the steps you can take to protect your information, by contacting your state Attorney General or the Federal Trade Commission. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580; www.ftc.gov/idtheft; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. Instances of known or suspected

identity theft should be reported to law enforcement, your Attorney General, and the FTC. You can also further educate yourself about placing a fraud alert or security freeze on your credit file by contacting the FTC or your state's Attorney General. This notice has not been delayed as a result of a law enforcement investigation.

For Maryland residents, the Maryland Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. Boys Town is located at: 14100 Crawford Street, Boys Town, NE 68010.

For North Carolina residents, the North Carolina Attorney General can be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General can be contacted by mail at 150 South Main Street, Providence, RI 02903; by phone at (401) 274-4400; and online at www.riag.ri.gov. You have the right to file and obtain a police report if you ever experience identity theft or fraud. A total of four (4) Rhode Island residents were impacted by this incident.

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 agencies 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 violators. 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. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should also be reported to law enforcement.

EXHIBIT C

Media Contact: Sian Schafle
(267) 930-4799

BOYS TOWN NATIONAL RESEARCH HOSPITAL PROVIDES NOTICE OF DATA BREACH

Boys Town, Nebraska (July 20, 2018) – Boys Town National Research Hospital ("Boys Town") is providing notice to current and former patients and employees of a recent incident involving personal information. To date, Boys Town has not received any reports that personal information has been misused as a result of this incident.

What Happened? On May 23, 2018, Boys Town became aware of unusual activity relating to an employee email account. Boys Town quickly launched an investigation to determine what may have happened and what information may have been affected, working together with computer forensics experts. The investigation determined that an unknown individual had access to the email account on May 23, 2018. Boys Town reviewed the email account to identify what personal information was stored within the email account. On or around July 3, 2018, Boys Town confirmed the personal information that may have been accessible as a result of the incident and the identities of the individuals relating to this personal information.

What Information Was Involved? The investigation in this matter confirmed that the following types of personal information related to Boys Town patients and employees may have been accessible as a result of the incident: name, date of birth, Social Security number, diagnosis or treatment information, Medicare or Medicaid identification number, medical record number, billing/claims information, health insurance information, disability code, birth or marriage certificate information, Employer Identification Number, driver's license number, passport information, banking or financial account number, and username and password. To date, Boys Town has not received any reports of the misuse of this information.

What is Boys Town Doing? Boys Town takes this incident and the security of personal information seriously. Upon learning of this incident, Boys Town moved quickly to confirm whether personal information may have been affected by this incident, to identify the individuals related to this personal information, to put in place resources to assist them, and to provide them with notice of this incident. Boys Town is reviewing its existing policies and procedures, and implementing additional safeguards to protect information stored in its systems. Boys Town reported this incident to law enforcement and is notifying state regulators, as required. Boys Town is also notifying potentially affected individuals and will be offering these individuals access to 12 months of free identity protection services.

What You Can Do? Boys Town encourages potentially impacted individuals to review their accounts, explanations of benefits, and credit reports for suspicious activity, and to report any suspicious activity to the affiliated institutions immediately. Boys Town is providing potentially impacted individuals with contact information for the three major credit reporting agencies, as well as providing advice on how to obtain free credit reports and how to place fraud alerts and security freezes on their credit files.

For More Information. Boys Town has set up a call center to answer questions from those who might be impacted by this incident. The call center can be reached at 1-855-686-9425 (toll free), Monday through Saturday, 8:00 a.m. to 8:00 p.m. CT. If you do not receive a letter in the coming weeks, but want to confirm whether you are affected, please contact the call center at the number listed above. Additional information can also be found at Boys Town's website, www.boystownhospital.org. Potentially affected individuals may also consider the information and resources outlined below.

Town encourages potentially impacted individuals to remain vigilant against incidents of identity theft and fraud by reviewing their accounts, explanations of benefits, and credit reports for suspicious activity, and to report any suspicious activity to the affiliated institutions immediately.

Media Contact: Sian Schafle
(267) 930-4799

Under U.S. law, individuals with credit reports are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Individuals may also contact the three major credit bureaus directly to request a free copy of their credit report. The credit reporting agencies may be contacted as follows:

Equifax	Experian	TransUnion
P.O. Box 105281	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-685-1111	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Potentially impacted individuals may also find information regarding identity theft, fraud alerts, security freezes and the steps they may take to protect their information by contacting the credit agencies, and the Federal Trade Commission. The Federal Trade Commission can 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 encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should be promptly reported to law enforcement, the Federal Trade Commission, and their state Attorney General. Individuals have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, they will likely need to provide some kind of proof that they have been a victim. This notice has not been delayed as the result of a law enforcement investigation. Credit file security freeze fees vary based on where you live, but commonly range from $0 to $15 each ($5 each in Massachusetts).

For North Carolina residents, the North Carolina Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at www.ncdoj.gov. **For Maryland residents**, the Maryland Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. Boys Town is located at 14100 Crawford Street, Boys Town, NE 68010. **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 agencies 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 Rhode Island residents**, the Attorney General can be contacted by mail at 150 South Main Street, Providence, RI 02903; by phone at (401) 274-4400; and online at www.riag.ri.gov. A total of four (4) Rhode Island residents were impacted by this incident.