

STATE OF MINNESOTA

DISTRICT COURT

COUNTY OF STEELE

THIRD JUDICIAL DISTRICT

Justin Hiatt, on behalf of himself
individually and all others similarly
situated,

Plaintiff,

v.

South Country Health Alliance, a Joint
Powers Board,

Defendant.

Court File No.: _____

Case Type: Breach of Contract;
Minnesota Government Data Practices Act

**CLASS ACTION COMPLAINT
AND JURY DEMAND**

Plaintiff Justin Hiatt (hereinafter “Mr. Hiatt” or “Plaintiff”) on behalf of himself and the proposed class defined below alleges as follows:

NATURE OF THE ACTION

1. This case is about the failure of a health plan, South Country Health Alliance, a Joint Powers Board (“SCHA”) to protect its members’ protected health information (“PHI”).
2. On or about June 25, 2020, SCHA’s email system was breached, and hackers gained access to the PHI of 66,874 members. SCHA notified victims of the Data Breach more than six months later, on or about December 30, 2020.
3. The compromised PHI includes but is not limited to members’ names, Social Security numbers, addresses, Medicare and Medicaid numbers, health insurance information, diagnostic or treatment information, dates of death (if applicable), provider name and treatment cost information.

4. Plaintiff is a former SCHAs plan member who became a victim of Defendant's insufficient data security practices. Plaintiff has suffered a tangible and concrete injury-in-fact.

5. Accordingly, Plaintiff, on his own behalf and on behalf of a class of similarly situated individuals, brings this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendant's possession.

THE PARTIES

6. Plaintiff Justin Hiatt is a natural person and citizen of the state of Minnesota, residing in Rochester, Minnesota.

7. Defendant, SCHAs is a Joint Powers Board created pursuant to a Joint Powers Agreement entered into between various Minnesota counties under Minn. Stat. § 471.59 in accordance with Minn. Stat. § 256B.692, formed to operate, control, and manage county-based purchasing functions for persons enrolled in public healthcare programs, which is headquartered in Owatonna, Minnesota.

JURISDICTION AND VENUE

8. This Court is vested with subject-matter jurisdiction pursuant to Minn. Const. art. VI, § 3 and Minn. Stat. § 484.01, subd. 1.

9. This Court has general personal jurisdiction over SCHAs because it is a Minnesota Joint Powers Board comprised of Minnesota counties, it maintains its principal place of business in Minnesota, and provides health insurance to Minnesota citizens.

10. Venue is proper in this Court pursuant to Minn. Stat. § 13.08 and §542.09 because Defendant's principal place of business is located in Owatonna, Minnesota, which the cause of action or some part thereof arose.

COMMON FACTUAL ALLEGATIONS

11. As stated, *ante*, Defendant SCHA is a Joint Powers Board which was formed to coordinate social service, public health, and medical services for the residents of certain Minnesota counties. At all times relevant hereto, SCHA provided health plan services to Wabasha County, Goodhue County, Brown County, Dodge County, Kanabec County, Sibley County, Steele County, Waseca County and Freeborn County Minnesota.

12. To provide its services, SCHA requires members to entrust it with their PHI—namely, their names, Social Security numbers, addresses, Medicare and Medicaid numbers, health insurance information, diagnostic or treatment information, provider name and treatment cost information.

13. SCHA maintains and stores its members' PHI.

14. On or about June 25, 2020, unauthorized actor(s) infiltrated one of SCHA's employee's email accounts in order to purloin the PHI of approximately 66,874 members (the "Data Breach").

15. On or about December 30, 2020, SCHA began notifying members of the Data Breach¹.

16. According to SCHA's Data Breach notice, "on September 14, 2020, SCHA discovered that unauthorized access to an employee email account had occurred on June 25, 2020." That same day, SCHA commenced an investigation, ultimately discovering that the PHI of 66,874 members "may have been in the account..." that was accessed.

17. According to the notice, SCHA determined that Plaintiff and the putative class's "names, Social Security numbers, addresses, Medicare and Medicaid numbers, health insurance

¹ SCHA's notice is annexed hereto as Plaintiff's Exhibit A.

information, diagnostic or treatment information, date of death, provider name, and treatment cost information...” “may have been involved in the incident”.

18. The notice encouraged SCHA members to call a dedicated toll-free line to answer patient questions.

19. The notice also advised members to “notify [their] financial institution immediately if [they] detect any suspicious activity on any of [their] accounts, including unauthorized transactions or new accounts opened in [SCHA’s] name that [they] do not recognize.”

20. Plaintiff and members of the Proposed Class are victims of the Data Breach who relied on SCHA to keep their PHI confidential and securely maintained.

21. SCHA was negligent in safeguarding the victims’ PHI because SCHA had repeated warnings and alerts of the increasing risk of general email scams and the actual scam it chose to ignore and to which it fell prey.

22. Business Email Compromise or spoofing is the forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual source. For example, spoofed email may purport to be from someone in a position of authority within a company asking for sensitive data such as passwords or employee information that can be used for a variety of criminal purposes. A telltale sign of a spoofing e-mail is an “urgent” request from a company “executive” requesting that confidential information be provided via email.

23. As noted by cybersecurity journalist Brian Krebs, this type of fraud “usually begins with the thieves either phishing an executive and gaining access to that individual’s email

account or emailing employees from a look-alike domain that is one or two letters off from the company's true domain name.”²

24. Over the past several years, data breaches have become alarmingly commonplace. In 2016, the number of data breaches in the U.S. exceeded 1,000, a 40% increase from 2015. The next year, that number increased by nearly 50%. The following year the healthcare sector was the second easiest “mark” among all major sectors and categorically had the most widespread exposure per data breach.

25. Healthcare data breaches have continued to rapidly increase. According to the 2019 Healthcare Information and Management Systems Society Cybersecurity Survey, 82 percent of participating healthcare providers reported having a significant security incident within the last 12 months, with a majority of those being caused by “bad actors.”

26. The healthcare industry has “emerged as a primary target because [it sits] on a gold mine of sensitive personally identifiable information for thousands of members at any given time. From social security and insurance policies to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers.”

27. The PHI stolen in the Data Breach is significantly more valuable than the loss of, say, credit card information in a large retailer data breach. Victims affected by those retailer breaches could avoid much of the potential future harm by simply cancelling credit or debit cards and obtaining replacements. The information stolen in the Data Breach—most notably name, date of birth and social security number—is difficult, if not impossible, to change.

² Brian Krebs, *FBI: \$2.3 Billion Lost to CEO Email Scams*, KREBS ON SECURITY, (April 7, 2016), available at <http://krebsonsecurity.com/2016/04/fbi-2-3-billion-lost-to-ceo-email-scams/> (last visited March 26, 2020).

28. PHI data for sale is so valuable because PHI is so broad, and it can therefore be used for various criminal activities, such as creating fake IDs, buying medical equipment and drugs that can be resold on the street, or combining patient numbers with false provider numbers to file fake claims with insurers.

29. As storehouses of that lucrative information, healthcare companies like SCHA are also highly targeted by cybercriminals because they lack “sufficient resources to prevent or quickly detect a data breach,” making them an easier target.

30. Cybercriminals regularly target the healthcare industry with email phishing schemes, which “remain[] the primary attack vector for nine out of 10 cyberattacks.” SCHA did not elaborate on how the Data Breach happened, other than a description that suggests it was a phishing attack.

31. Companies can mount two primary defenses to phishing scams: employee education and technical security barriers.

32. Employee education is the process of adequately making employees aware of common phishing attacks and implementing company-wide policies requiring the request or transfer of sensitive personal or financial information to known recipients through secure sources. Employee education and secure file-transfer protocols provide the easiest method to assist employees in properly identifying fraudulent e-mails and preventing unauthorized access to PHI.

33. From a technical perspective, companies can also greatly reduce the flow of phishing e-mails by implementing certain security measures governing e-mail transmissions. Companies can use a simple email validation system that allows domain owners to publish a list of IP addresses that are authorized to send emails on their behalf to reduce the amount of spam and fraud by making it much harder for malicious senders to disguise their identities. Companies can

also use email authentication, which serves to block email streams that have not been properly authenticated.

34. SCHA failed to adequately train its employees on even the most basic of cybersecurity protocols, including:

- a. How to detect phishing emails and other scams, including providing employees examples of these scams and guidance on how to verify if emails are legitimate;
- b. Effective password management and encryption protocols for internal and external emails;
- c. Avoidance of responding to emails that are suspicious or from unknown sources;
- d. Locking, encrypting, and limiting access to computers and files containing sensitive information;
- e. Implementing guidelines for maintaining and communicating sensitive data; and
- f. Protecting sensitive patient information, including personal and financial information, by implementing protocols on how to request and respond to requests for the transfer of such information and how to securely send such information through a secure file transfer system to only known recipients.

35. The Data Breach was caused by SCHA's violation of its obligation to abide by best practices and industry standards concerning the security of its computer and email systems. SCHA failed to comply with security standards and allowed its victims' PHI to be stolen by failing to implement security measures that could have prevented or mitigated the Data Breach.

36. SCHA failed to ensure that all personnel were made aware of this well-known and well-publicized phishing email scam.

The Data Breach and Notice

37. SCHA admitted to the breach on or about December 30, 2020 in a notice.

38. The notice recommended that members notify their financial institutions “immediately” if they notice any “suspicious” or “unauthorized” activity on their accounts, including new accounts opened in SCHA’s name that they do not recognize.

39. SCHA did not identify a single action it took to increase security and protect Plaintiff’s PHI going forward.

PHI was Stolen and Defendant Immediately Recognized the Risk of Identity Theft

40. The gravamen of this lawsuit is that SCHA failed to keep Plaintiff’s and the Class Members’ PHI confidential, whether knowingly and willfully or negligently, as required by law, and that Plaintiff and the Class Members have suffered legally cognizable concrete and tangible injury as a result. There is a high and substantial likelihood that Plaintiff’s and the Class Members’ stolen PHI is being misused by cyber-criminals right now, and that misuse will be ongoing and without authorization. Plaintiff and Class Members therefore have incurred significant out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud.

41. SCHA recognized the actual imminent harm and injury that flowed from the Data Breach, so it recommended that Plaintiff and Class Members “please notify [their] financial institution immediately” if they detect charges for services that were not received, even those purporting to originate from SCHA.

42. SCHA also offered members complimentary identify monitoring services.

43. Even with complimentary identity-theft protection, the risk of identity theft and unauthorized use of Plaintiff’s and Class Members’ PHI is still substantially high.

44. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and Class Member's PHI. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and Class Members' financial accounts.

45. The act of stealing or improperly accessing Plaintiff's and the Class Members' PHI, and the cyber-criminals' purpose in stealing Plaintiff's and the Class Members' PHI, was to commit additional illegal acts and crimes, such as generating fraudulent charges with Plaintiff's and the Class Members' financial accounts, gaining unauthorized access to their internet accounts, opening unauthorized financial accounts, and both financial and medical identity theft, among other criminal activity. Theft of PHI necessarily implies harm because the misuse of data is the only plausible explanation for the Data Breach.

46. In a recent survey³ conducted by the Medical Identity Fraud Alliance (MIFA), a healthcare industry trade group, 52 percent of victims said their information was used to obtain government benefits like Medicare or Medicaid. And 59 percent had their identity used to obtain healthcare, while 56 percent said a scammer parlayed their data into prescription drugs or medical equipment.

47. This type of injury and harm, including actual fraud, is directly traceable to the Data Breach. This harm is not just possible, not just certainly impending, it has happened and is *ongoing*, and all Class Members are in imminent and immediate danger of being further subjected to this injury.

³ *Fifth Annual Study on Medical Identity Theft*, MED. IDENTITY FRAUD ALLIANCE, (Feb. 2015), available at http://www.medidfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_Theft_Study1.pdf (last visited March 26, 2020).

48. The ramifications of SCHA's failure to keep its victims' PHI secure are long lasting and severe. Once PHI is stolen, fraudulent use of that information and damage to victims may continue for years.

49. The fraudulent activity resulting from the Data Breach may not come to light for years.

50. Despite all of the publicly available knowledge of PHI being compromised and alerts regarding the phishing email scam perpetrated, SCHA's approach to maintaining the privacy of its victims' PHI was lackadaisical, cavalier, reckless, or in the very least, negligent.

51. SCHA has failed to compensate Plaintiff and Class Members victimized in this Data Breach. Upon information and belief, SCHA has not offered to provide assistance or compensation for the costs and burdens — current and future — associated with the identity theft and fraud resulting from the Data Breach. SCHA has not offered victims of the Data Breach any assistance in dealing with the IRS, the state tax agencies, or any of the three major credit-reporting agencies.

52. It is incorrect to assume that reimbursing a victim of the Data Breach for financial loss due to fraud makes that individual whole again. On the contrary, after conducting a study, the U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."⁴

⁴ Victims of Identity Theft, 2012 (Dec. 2013) at 10, 11, available at <https://www.bis.gov/content/pub/pdf/vit12.pdf> (last visited April 11, 2018).

53. As a result of SCHA's failure to prevent the Data Breach, Plaintiff and Class Members have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at increased risk of suffering:

- a. The loss of the opportunity to control how their PHI is used;
- b. The diminution in value of their PHI;
- c. The compromise, publication and/or theft of their PHI;
- d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;
- e. Lost opportunity costs and lost wages associated with the time and effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;
- f. Delay in receipt of tax refund monies;
- g. Unauthorized use of stolen PHI;
- h. The continued risk to their PHI, which remains in the possession of SCHA and is subject to further breaches so long as SCHA fails to undertake appropriate measures to protect the PHI in their possession; and
- i. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

54. Stolen PHI is a one of the most valuable commodities on the criminal information black market. In 2014, the FBI warned healthcare organizations that PHI data is worth 10 times as

much as personal credit card data on the black market.⁵ PHI data for sale is so valuable because PHI information is so broad, and it can therefore be used for a wide variety of criminal activity such as: to create fake IDs, buy medical equipment and drugs that can be resold on the street, or combine patient numbers with false provider numbers to file fake claims with insurers.

55. The value of Plaintiff's and the Class Members' PHI on the black market is considerable. Stolen PHI trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" Internet websites, making the information publicly available, for a substantial fee of course.

56. It can take victims years to spot identity or PHI theft, giving criminals plenty of time to milk that information for cash. That is precisely what makes PHI more desirable to criminals than credit card theft. Credit card theft can be spotted by banks early on, and accounts can be quickly frozen or cancelled once the fraud is detected, making credit card data much less valuable to criminals than PHI.

57. SCHA disclosed the PHI of Plaintiff and the Class Members for criminals to use in the conduct of criminal activity. Specifically, SCHA opened up, disclosed, and exposed the PHI of Plaintiff and the Class Members to persons engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and

⁵ Stolen PHI health credentials can sell for up to 20 times the value of a U.S. credit card number, according to Don Jackson, director of threat intelligence at PhishLabs, a cyber-crime protection company who obtained his data by monitoring underground exchanges where cyber-criminals sell the information. See Humer, Caroline & Finkle, Jim, *Your medical record is worth more to hackers than your credit card*, REUTERS, (Sep. 24, 2014), <https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924> (last visited March 26, 2020). Dark web monitoring is a commercially available service which, at a minimum, Defendant can and should perform (or hire a third-party expert to perform).

fraudulent attempts to open unauthorized financial accounts (*i.e.*, identity fraud), all using the stolen PHI.

58. SCHA's use of outdated and unsecured computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up-to-date technology security strategy, demonstrates a willful and conscious disregard for healthcare patient privacy, and has exposed the PHI of Plaintiff and thousands of Class Members to unscrupulous operators, con artists, and outright criminals.

PLAINTIFF'S EXPERIENCE

59. Plaintiff Justin Hiatt is a resident of Rochester, Minnesota. He is a former member of SCHA.

60. As a condition for membership with SCHA, Plaintiff was required to make available to SCHA, its agents, and its employees, sensitive and confidential PHI, including, but not limited to, his name, Social Security number, address, Medicare and Medicaid number, health insurance information, diagnostic or treatment information, provider name and treatment cost information.

61. SCHA acquires, collects, and stores a massive amount of PHI from its members, including Plaintiff.

62. By obtaining, collecting, using, and deriving a benefit from Plaintiff's PHI, SCHA assumed legal and equitable duties to those individuals and knew or should have known that it was responsible for protecting their PHI from unauthorized disclosure.

63. Plaintiff has taken reasonable steps to maintain the confidentiality of his PHI.

64. Plaintiff relied on SCHA to keep his PHI confidential and securely maintained, to use this information for business purposes only, and to take reasonable steps to ensure that SCHA's vendors would make only authorized disclosures of this information.

65. Indeed, SCHA maintains a policy, and gives a copy to its members, which specifically acknowledges its legal obligation to maintain the privacy of patient PHI entrusted to it and to control the disclosure thereof.

66. SCHA's privacy policy is outlined in its Notice of Privacy Practices (SCHA's "Privacy Policy"), which was effective on March 1, 2015.⁶

67. In its Privacy Policy, SCHA represents that it "has always been committed to maintaining the security and confidentiality of the information [it receives] from [its] members." The Privacy Policy goes on to say "[w]hether it's your medical information or identifiable information (name, address, phone number, or member identification number), we maintain careful safeguards to protect [members] against unauthorized access and use." SCHA advises its members they "can be assured that every effort is taken to comply with federal and state laws, rules and regulations – physically, electronically, and procedurally – to safeguard your information."

68. SCHA further represents that it is "required by law" to maintain the privacy of members' PHI.

69. The Privacy Policy states that SCHA, *inter alia*:

- a. Is required to follow the Privacy Policy.
- b. Is required to give members a copy of the Privacy Policy.
- c. Is required to notify members in the event of a data breach.

⁶ SCHA's Privacy Policy is annexed hereto as Plaintiff's Exhibit B.

d. If SCHA's privacy practices change it will send a new notice before the change becomes effective.

e. Requires all employees, business associates, providers, and vendors to adhere to its Privacy Policy under its "strictest standards."

70. SCHA's Privacy Policy describes the ways in which members' PHI can be disclosed to third parties.

71. It states how PHI can be shared with third parties for Treatment, Health Care Operations, Payment, and other purposes.

72. The Privacy Policy also describes how PHI can be used for research, so long as "certain established measures are taken to protect [members'] privacy."

73. In a nutshell, SCHA's Privacy Policy limited the circumstances in which Plaintiff's PHI could be disclosed to third parties and delineated the responsibilities of SCHA in securing that PHI.

74. SCHA failed to honor the terms of the Privacy Policy when it disclosed Plaintiff's PHI to third parties not listed in the Privacy Policy.

75. SCHA also failed to honor the terms of the Privacy Policy by failing to adequately safeguard that PHI.

76. In short, the Data Breach was not permitted by SCHA's Privacy Policy.

77. Plaintiff entrusted his PHI to SCHA solely for the purpose of health plan membership with the expectation and implied mutual understanding that SCHA would strictly maintain the confidentiality of the PHI and safeguard it from theft or misuse.

78. Plaintiff would not have entrusted SCHA with his PHI had he known SCHA would fail to take adequate steps to secure its computer and email systems.

79. Plaintiff and every member of his family received a separate letter from SCHA (the “Notice Letter”) notifying them of the Data Breach. The Notice Letter informed Plaintiff and his family that they were a victim of the Data Breach and that their PHI was compromised.

80. As a result of the Data Breach, Plaintiff must expend considerable time and effort monitoring his accounts to protect himself from additional identity theft. Moreover, Plaintiff has been forced to purchase identity theft protection services with LifeLock in order to mitigate the increased risk of identity theft he has been exposed to.

81. Aside from the financial loss consequences, both direct and indirect, that Plaintiff is more than likely to face, identity theft negatively impacts credit scores.⁷ Because a criminal’s delinquent payments, cash loans, or even foreclosures slowly manifest into weakened credit scores, and because this type of fraud takes the longest time to resolve, Plaintiff is forced to subscribe to a credit monitoring service for the indefinite future.

82. Indeed, Plaintiff has discovered that shortly after the Data Breach, in approximately August of 2020, Chase bank accounts were opened using his compromised PHI in Germany and Australia.

83. Plaintiff has opened no such bank accounts in either Germany or Australia.

84. Plaintiff has received additional emailed receipts for purchases made with those bank accounts as recently as this year.

⁷ Direct financial loss refers to the amount of money stolen or misused by the identity theft offender. Indirect financial loss includes any outside costs associated with identity theft, like legal fees or overdraft charges. A 2014 Department of Justice study found that victims experienced a combined average loss of \$1,343.00. In total, identity theft victims lost a whopping \$15.4 billion in 2014 alone. *See* Gredler, Cody, *The Real Cost of Identity Theft*, CSIDENTITY, (Sep. 9, 2016), <https://www.csid.com/2016/09/real-cost-identity-theft/> (last visited March 26, 2020).

85. It can take years to spot identity or PHI theft. Even if SCHA offered Plaintiff a lifetime subscription to a credit monitoring service, Plaintiff would be powerless to prevent identity theft.

86. As previewed above, as the amount of information from both unregulated sources that have identities and addresses attached (*i.e.*, phone books, search engines, and websites) and illegal sources (*i.e.*, stolen information like the PHI) grows over time, there is more and more information about who people might be. As a result, cyber-criminals can cross-reference these two sources to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as “Fullz” packages.⁸

87. These techniques mean that the PHI stolen in the Data Breach can easily be used to link and identify it to Plaintiff’s and the Class Members’ phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even though certain information such as emails, phone numbers, credit card numbers, or social security numbers, may not be included in the PHI stolen by the cyber-criminals in the Data Breach, they can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam

⁸ “Fullz” is fraudster speak for data that includes the *full* information of the victim, including name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to \$100 per record or more on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even “dead Fullz”, which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a “mule account” (an account that will accept a fraudulent money transfer from a compromised account) without the victim’s knowledge. *See, e.g.*, Brian Krebs, *Medical Records For Sale in Underground Stolen From Texas Life Insurance Firm*, KREBS ON SECURITY, (Sep. 18, 2014), available at <https://krebsonsecurity.com/tag/fullz/> (last visited March 26, 2020).

telemarketers) over and over. That is exactly what has happened or is likely to happen to Plaintiff and the Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to so find.

88. Identity theft is not only impacting Plaintiff and Class Members financially, but it is taking a significant emotional and physical toll. Plaintiff and other Class Members, like other PHI theft victims, fear for their personal financial security and are experiencing feelings of rage and anger, anxiety, sleep disruption, stress, fear, and physical pain.

89. This goes far beyond allegations of mere worry or inconvenience; the injury and harm to a Data Breach victim is the type contemplated and addressed by law.

CLASS ALLEGATIONS

90. Pursuant to Minn. R. Civ. Proc. 23, Plaintiff brings this class action on behalf of himself and the following proposed Class (the “Class”):

All citizens of Minnesota whose PHI was compromised as a result of the Data Breach with SCHA which was announced by SCHA on or about December 30, 2020.

91. The following people are excluded from the Class: (1) any judge or magistrate presiding over this action and members of their families; (2) Defendant, Defendant’s subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which the Defendant or its parent has a controlling interest, and their current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff’s counsel and Defendant’s counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

92. Plaintiff and the Class Members satisfy the numerosity, commonality, typicality, adequacy, and predominance prerequisites for suing as representative parties pursuant to Rule 23.01.

93. **Numerosity:** The exact number of Class members is unknown but is estimated to be at least 66,874 persons at this time, and individual joinder in this case is impracticable. Class Members can be easily identified through Defendant's records and objective criteria permitting self-identification in response to notice, and notice can be provided through techniques similar to those customarily used in other data breach, consumer breach of contract, unlawful trade practices, and class action controversies.

94. **Typicality:** Plaintiff's claims are typical of the claims of other Class members in that Plaintiff, and the Class Members sustained damages arising out of Defendant's Data Breach, wrongful conduct and misrepresentations, false statements, concealment, and unlawful practices, and Plaintiff and the Class Members sustained similar injuries and damages, as a result of Defendant's uniform illegal conduct.

95. **Adequacy:** Plaintiff will fairly and adequately represent and protect the interests of the Class and has retained counsel competent and experienced in complex class actions to vigorously prosecute this action on behalf of the Class. Plaintiff has no interests that conflict with, or are antagonistic to those of, the Class, and Defendant has no defenses unique to Plaintiff.

96. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiff and the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include, but are not necessarily limited to the following:

- a. whether Defendant breached its contractual promises to safeguard Plaintiff's and the Class Members' PHI;
- b. whether Defendant knew or should have known about the inadequacies of its data security policies and system and the dangers associated with storing sensitive PHI;
- c. whether Defendant failed to use reasonable care and commercially reasonable methods to safeguard and protect Plaintiff's and the other Class Members' PHI from unauthorized release and disclosure;
- d. whether the proper data security measures, policies, procedures, and protocols were in place and operational within Defendant's computer and software systems to safeguard and protect Plaintiff's and the other Class Members' PHI from unauthorized release and disclosure;
- e. whether Defendant took reasonable measures to determine the extent of the Data Breach after it was discovered;
- f. whether Defendant's delay in informing Plaintiff and the other Class Members of the Data Breach was unreasonable;
- g. whether Defendant's method of informing Plaintiff and the other Class Members of the Data Breach was unreasonable;
- h. whether Plaintiff and the Class Members were damaged as a proximate cause or result of Defendant's breach of its contract with Plaintiff and the Class Members;
- i. whether Defendant's practices and representations related to the Data Breach that compromised the PHI breached implied warranties;
- j. what the proper measure of damages is; and

- k. whether Plaintiff and the Class Members are entitled to restitutionary, injunctive, declaratory, or other relief.

97. **Superiority:** This case is also appropriate for class certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy as joinder of all parties is impracticable. The damages suffered by the individual members of the Class will likely be relatively small, especially given the burden and expense of individual prosecution of the complex litigation necessitated by Defendant's actions. Thus, it would be virtually impossible for the individual members of the Class to obtain effective relief from Defendant's misconduct. Even if members of the Class could sustain such individual litigation, it would still not be preferable to a class action, because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Economies of time, effort and expense will be fostered, and uniformity of decisions ensured.

98. A class action is therefore superior to individual litigation because:

- a. the amount of damages available to an individual plaintiff is insufficient to make litigation addressing Defendant's conduct economically feasible in the absence of the class action procedural device;
 - b. individualized litigation would present a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system;
- and

- c. the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

99. In addition to satisfying the prerequisites of Rule 23.01, Plaintiff satisfies the requirements for maintaining a class action under Rule 23.02 because:

- a. the prosecution of separate actions by the individual Class Members would create a risk of inconsistent or varying adjudication which would establish incompatible standards of conduct for Defendant;
- b. the prosecution of separate actions by individual Class Members would create a risk of adjudications with respect to them which would, as a practical matter, be dispositive of the interests of other Class Members not parties to the adjudications, or substantially impair or impede their ability to protect their interests;
- c. Defendant has acted or refused to act on grounds that apply generally to the proposed Class, thereby making final injunctive relief or declaratory relief herein appropriate with respect to the proposed Class as a whole; and
- d. questions of law or fact common to the members of the class predominate over any questions affecting only individual members, and that a class action is superior to other available methods for the fair and efficient adjudication of the controversy.

COUNT I

Breach of Contract against Defendant On Behalf of Plaintiff and the Class

100. Plaintiff and the Class Members incorporate the above allegations as if fully set forth herein.

101. Defendant offered to provide health plan services to Plaintiff and Class Members.

102. Plaintiff and Class Members accepted Defendant's offer to provide health plan services by signing up for and receiving same.

103. Defendant required Plaintiff and Class Members to provide their PHI including members' names, Social Security numbers, addresses, Medicare and Medicaid numbers, health insurance information, diagnostic or treatment information, provider name and treatment cost information in order to participate in Defendant's health plan.

104. The Parties' agreement was supported by adequate consideration because Plaintiff and Class Members entrusted their PHI to SCHA, received health insurance and coordination of care benefits from SCHA and sought preventative and remedial healthcare treatment using those benefits, while under no legal obligation to do so.

105. In its Privacy Policy, which was incorporated into the Parties' agreement by reference, Defendant expressly promised Plaintiff and the Class Members that Defendant would only disclose PHI under certain circumstances, none of which relate to the Data Breach.

106. Necessarily implicit in the agreement between Defendant and its members, including Plaintiff and Class members, was Defendant's obligation to use such PHI for business and treatment purposes only, to take reasonable steps to secure and safeguard that PHI, and not make disclosures of the PHI to unauthorized third parties.

107. Further implicit in the agreement, Defendant was obligated to provide Plaintiff and the Class Members with prompt and adequate notice of any and all unauthorized access and/or theft of their PHI.

108. Plaintiff and the Class Members would not have entrusted their PHI to Defendant in the absence of such agreement with Defendant.

109. Defendant materially breached the express and/or implied, unilateral and/or bilateral contract(s) it had entered with Plaintiff and Class Members by failing to safeguard such information and failing to notify them promptly of the intrusion into its computer systems that compromised such information. Defendant further breached the implied contracts with Plaintiff and Class members by:

- a. Failing to properly safeguard and protect Plaintiff's and Class Members' PHI;
- b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement;
- c. Failing to ensure the confidentiality and integrity of electronic PHI that Defendant created, received, maintained, and transmitted in violation of 45 C.F.R. § 164.306(a)(1).

110. The damages sustained by Plaintiff and Class Members as described above were the direct and proximate result of Defendant's material breaches of its agreements.

111. Plaintiff and Class Members have performed as required under the relevant agreements, or such performance was waived by the conduct of Defendant.

112. Under the laws of Minnesota, good faith is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

113. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

114. Defendant failed to promptly advise Plaintiff and Class Members of the Data Breach.

115. In these and other ways, Defendant violated its duty of good faith and fair dealing.

116. Plaintiff and Class Members have sustained damages as a result of Defendant's breaches of its agreement, including breaches thereof through violations of the covenant of good faith and fair dealing.

COUNT II
Promissory Estoppel
On Behalf of Plaintiff and the Class against Defendant

117. Plaintiff and the Class Members incorporate the above allegations as if fully set forth herein.

118. Plaintiff pleads this theory in the alternate to his breach of contract count, *ante*.

119. As more fully explained, *ante*, SCHA made multiple clear and definite promises that it would safeguard Plaintiff's and Class Members' PHI if entrusted to it, contained in SCHA's Privacy Policy and elsewhere.

120. SCHA intended for Plaintiff and Class Members to rely upon its promises, and they reasonably did so to their detriment by entrusting SCHA with their PHI.

121. In the event no enforceable obligation arises from the expressions or the conduct of the Parties *vis-à-vis* the security of PHI, SCHA's promises to safeguard PHI must be enforced by this Court to prevent injustice.

122. It would be in the public interest to hold a public entity such as SCHAs to the promises it made to its members to safeguard their PHI.

123. Plaintiff and Class Members have sustained damages as a result of Defendant's breaches of its promises to safeguard Plaintiff's and Class Members' PHI.

COUNT III
Minnesota Government Data Practices Act ("MGDPA")
Minn. Stat. §§ 13.01, *et seq.*
On Behalf of Plaintiff and the Class against Defendant

124. Plaintiff and the Class Members incorporate the above allegations as if fully set forth herein.

125. Plaintiffs and the Class Members are "Individuals" within the meaning of Minn. Stat. § 13.02, subd. 8.

126. Plaintiffs' and Class Members' PHI is "Data on individuals", "Nonpublic data" and "Private data on individuals" within the meaning of Minn. Stat. §§ 13.02, subs. 5, 9, 12.

127. Defendant is both a "Government entity" and a "Political subdivision" within the meaning of Minn. Stat. §§ 13.02, subs. 7a, 11.

128. Minn. Stat. § 13.05, subd. 3 provides that "Collection and storage of all data on individuals and the use and dissemination of private and confidential data on individuals shall be limited to that necessary for the administration and management of programs specifically authorized by the legislature or local governing body or mandated by the federal government..." and Minn. Stat. § 13.05, subd. 4, provides that "Private or confidential data on an individual shall not be collected, stored, used, or disseminated by government entities for any purposes other than those stated to the individual at the time of collection in accordance with section 13.04, except as provided" therein.

129. Suffice it to say, that subdivision does not countenance a disclosure of Plaintiff's and Class Members' PHI like the Data Breach.

130. Moreover, subdivision 5 of that section provides that "The responsible authority shall: ... establish appropriate security safeguards for all records containing data on individuals, including procedures for ensuring that data that are not public are only accessible to persons whose work assignment reasonably requires access to the data, and is only being accessed by those persons for purposes described in the procedure; and []develop a policy incorporating those procedures, which may include a model policy governing access to the data if sharing of the data with other government entities is authorized by law..." Minn. Stat. §§ 13.05, subs. 5(2)-(3).

131. Upon information and belief, SCHA did not establish appropriate security safeguards for Plaintiff's and Class Members' PHI, as more fully detailed, *ante*, which ultimately resulted in the Data Breach that came to pass.

132. Moreover, Minn. Stat. § 13.055 requires government entities, such as SCHA, to disclose any "Breach of the security of the data", such as the Data Breach, to individuals affected thereby "in the most expedient time possible without unreasonable delay...", and SCHA did not.

133. As more fully explained, *ante*, SCHA has violated the aforesaid provisions of the MGDPA.

134. Minn. Stat. § 13.08 provides for a private action for damages, injunctive relief, costs, and reasonable attorney fees for the violation of any provision of that chapter, and explicitly waives any immunity to such a cause of action.

135. As more fully explained, *ante*, Plaintiff has suffered identity theft due to the Data Breach, he has expended money to purchase identity theft protection with LifeLock as a result of the Data Breach and he has also suffered emotional distress and mental anguish due to his PHI

being exposed to cybercriminals, who have since used it to make fraudulent purchases and commit identity theft.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the proposed Class, requests that the Court:

A. Certify this case as a Class action on behalf of the Class defined above, appoint Plaintiff Justin Hiatt as Class representative, and appoint the undersigned as Class counsel;

B. Award declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class Members;

C. Award injunctive relief as is necessary to protect the interests of Plaintiff and the Class Members;

D. Enter an award in favor of Plaintiff and the Class Members that includes compensatory, exemplary, punitive damages, and statutory damages, including pre- and post-judgment interest thereon, in an amount to be proven at trial;

E. Award restitution and damages to Plaintiff and the Class Members in an amount to be determined at trial;

F. Enter an award of attorneys' fees and costs, as allowed by law;

G. Enter an award of pre-judgment and post-judgment interest, as provided by law;

H. Grant Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

I. Grant such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: April 22, 2021

Respectfully submitted,

HELLMUTH & JOHNSON PLLC

By: 

Nathan D. Prosser (#0329745)

Anne T. Regan (#0333852)

8050 West 78th Street

Edina, MN 55439

(952) 941-4005

nprosser@hjlawfirm.com

aregan@hjlawfirm.com

**BRANSTETTER STRANCH &
JENNINGS PLLC**

J. Gerard Stranch IV*

Peter Jannace*

515 Park Avenue

Louisville, KY 40208

(615) 254-8801

gerards@bsjfirm.com

peterj@bsjfirm.com

COHEN & MALAD, LLP

Lynn A. Toops*

One Indiana Square

Suite 1400

Indianapolis, Indiana 46204

(317) 214-0321

ltoops@cohenandmalad.com

LINVILLE JOHNSON PLLC

Christopher D. Jennings*

610 President Clinton Avenue

Suite #300

Little Rock, AR 72201

(501) 209-7777

chris@yourattorney.com


*Attorneys for Plaintiff and Putative
Class Members*

**pro hac vice forthcoming*

ACKNOWLEDGEMENT

The undersigned hereby acknowledges that costs, disbursements, and reasonable attorneys' and witness fees may be awarded pursuant to Minn. Stat. § 549.211, to the parties against whom the allegations in this pleading are asserted.

Dated: April 22, 2021



Nathan D. Prosser (#329745)

EXHIBIT A

South Country Health Alliance Notifies Consumers of Data Security Incident

OWATONNA, Minnesota--December 30, 2020--South Country Health Alliance (“SCHA”) has become aware of a data security incident that may have involved the personal information of some SCHA community members. SCHA has sent notification about this incident to potentially impacted individuals and has provided resources to assist them.

On September 14, 2020, SCHA discovered that unauthorized access to an employee email account had occurred on June 25, 2020. SCHA immediately secured the account, began an investigation, and engaged cybersecurity experts to assist with the investigation. On November 5, 2020, following a review of the contents of the email account, SCHA determined that personal information belonging to some SCHA community members may have been in the account. In response to learning this, SCHA took steps to identify current mailing addresses for the potentially impacted individuals so that SCHA could notify them and offer them complimentary credit monitoring and identity protection services.

Based on the investigation of the incident, the following personal and protected health information may have been involved in the incident: names, Social Security numbers, addresses, Medicare and Medicaid numbers, health insurance information, diagnostic or treatment information, date of death, provider name, and treatment cost information.

While SCHA is not aware of the misuse of any information impacted by this incident, on December 30, 2020, SCHA sent notice about this incident to potentially impacted members. Those letters provided information about the incident and about steps they can take to protect their personal information. SCHA also offered complimentary credit monitoring and identity protection services to potentially impacted members.

SCHA has established a toll-free call center to answer questions about the incident and to help impacted members enroll in complimentary credit monitoring and identity protection services. Call center representatives are available Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time and can be reached by calling 1-833-920-3172.

The privacy and protection of personal and protected health information is a top priority for SCHA, which deeply regrets any inconvenience or concern this incident may cause.

While we have no evidence of the misuse of any potentially affected individual's information, we are providing the following information to help those wanting to know more about steps they can take to protect themselves and their personal information:

What steps can I take to protect my personal information?

- Please notify your financial institution immediately if you detect any suspicious activity on any of your accounts, including unauthorized transactions or new accounts opened in our name that you do not recognize. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities.

- You can request a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies. To do so, free of charge once every 12 months, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting agencies is listed at the bottom of this page.
- You can take steps recommended by the Federal Trade Commission to protect yourself from identify theft. The FTC's website offers helpful information at www.ftc.gov/idtheft.
- Additional information on what you can do to better protect yourself is included in your notification letter.

How do I obtain a copy of my credit report?

You can obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies. To order your credit report, free of charge once every 12 months, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Use the following contact information for the three nationwide credit reporting agencies:

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-685-1111
www.equifax.com

How do I put a fraud alert on my account?

You may consider placing a fraud alert on your credit report. This fraud alert statement informs creditors to possible fraudulent activity within your report and requests that your creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact Equifax, Experian or TransUnion and follow the Fraud Victims instructions. To place a fraud alert on your credit accounts, contact your financial institution or credit provider. Contact information for the three nationwide credit reporting agencies is included in the letter and is also listed at the bottom of this page.

How do I put a security freeze on my credit reports?

You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, or regular stamped mail, or online by following the instructions found at the websites listed below. You will need to provide the following information when requesting a security freeze (note that if you are making a request for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) address. You may also be asked to provide other personal information such as your email address, a copy of a government-issued identification card, and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. There is no charge to place, lift, or remove

a freeze. You may obtain a security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze	Experian Security Freeze	TransUnion (FVAD)
PO Box 105788	PO Box 9554	PO Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
1-800-685-1111	1-888-397-3742	1-800-909-8872
www.equifax.com	www.experian.com	www.transunion.com

Minnesota Residents: A report discussing the facts of this incident and the results of the investigation has been prepared and will be made available to you upon request. If you would like a copy of the report, please call 1-833-920-3172 and tell the call center representative that you would like a copy of the report. In order for us to fulfill your request, you will be required to provide a mailing address or an email address to the call center representative.

What should I do if my family member was involved in the incident and is deceased?

You may choose to notify the three major credit bureaus, Equifax, Experian and Trans Union, and request they flag the deceased credit file. This will prevent the credit file information from being used to open credit. To make this request, mail a copy of your family member's death certificate to each company at the addresses below.

Equifax

Equifax Information
Services
P.O. Box 105169,
Atlanta, GA 30348

Experian

Experian Information
Services
P.O. Box 9701
Allen, TX 75013

TransUnion

Trans Union Information
Services
P.O. Box 2000
Chester, PA 19022

EXHIBIT B



Notice of Privacy Practices

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

Effective March 1, 2015

South Country Health Alliance (SCHA) has always been committed to maintaining the security and confidentiality of the information we receive from our members. Whether it's your medical information or identifiable information (name, address, phone number, or member identification number), we maintain careful safeguards to protect you against unauthorized access and use.

We are required by law to maintain the privacy of your personal health information and to provide this notice to you. We are also required to notify you of any breach of unsecured protected health information, should it occur. If our privacy practices change we will send you a new notice before we make a significant change in our practices. We hope this notice will clarify our responsibilities to you and provide you with a good understanding of your rights.

How SCHA safeguards your health information

Our privacy officer has the responsibility to implement and enforce privacy policies and procedures to protect your personal health information. You can be assured that every effort is taken to comply with federal and state laws, rules and regulations – physically, electronically, and procedurally – to safeguard your information. In some situations, where a state law provides greater protection for your privacy, we will follow the provisions of that state law.

SCHA requires all employees, business associates, providers and vendors to adhere to our privacy policies and procedures under our strictest standards. Following are descriptions of how your personal health information is handled throughout our administration of your health plan.

Permitted handling of health information

At SCHA, your personal health information is handled in a number of different ways as we administer your health plan benefits. The following examples show you the various uses we are permitted by law to make without your authorization:

Treatment. We may disclose your personal health information to health care providers (doctors, dentists, pharmacies, hospitals and other caregivers) who request it to aid in your treatment. We may also disclose your personal health information to these health care providers in an effort to provide you with preventive health, early

detection and disease and case management programs.

Payment. To administer your health benefits, policy or contract, we must use and disclose your health information to determine:

- Eligibility
- Claims payment
- Utilization and management of your benefits
- Medical necessity of your treatment
- Coordination of your care, benefits and other services
- Responses to complaints, appeals and external review requests

We may also use and disclose your health information to determine premium costs, underwriting, rates, and cost-sharing amounts. However, SCHA is prohibited from using or disclosing your protected health information that is genetic information for underwriting purposes.

Health care operations. To perform our health plan functions, we may use and disclose your health information to provide the following programs and evaluations:

- Health improvement or health care cost reduction programs
- Competence or qualification reviews of health care professionals
- Fraud and abuse detection and compliance programs
- Quality assessment and improvement activities
- Performance measurement and outcome assessments, health claims analysis and health services outreach
- Case management, disease management and care coordination services

We may also disclose your health information to SCHA affiliates and business associates that perform payment activities and conduct health care operations for us on your behalf.

Service reminders. We may contact you to remind you to obtain preventive health services or to inform you of treatment alternatives and/or health-related benefits and services, which may be of interest to you.

Additional uses and disclosures

In certain situations, the law permits us to use or disclose your personal health information without your authorization. These situations include:

Required by law. We may use or disclose your personal health information, as required to do so by state or federal law, including disclosures to the U.S. Department of Health and Human Services. Also, we are required to disclose your personal health information to you in accordance with the law.

Public health issues. We may disclose your health information to an authorized public health authority for public health activities in controlling disease, injury or disability. For example, we may disclose your personal health information to the childhood immunization registry.

Abuse or neglect. We may make disclosures to government authorities concerning abuse, neglect or domestic violence as required by law.

Health oversight activities. We may disclose your health information to a government agency authorized to conduct health care system or governmental procedures such as audits, examinations, investigations, inspections and licensure activity.

Legal proceedings. We may disclose your health information in the course of any legal proceeding, in response to a court order or administrative judge and, in certain cases, in response to a subpoena, discovery request or other lawful process.

Law enforcement. We may disclose your health information to law enforcement officials. For example, disclosures may be made in response to a warrant or subpoena or for the purpose of identifying or locating a suspect, witness or missing persons or to provide information concerning victims of crimes.

Coroners, medical examiners, funeral directors and organ donations. We may disclose your health information in certain instances to coroners and medical examiners during their investigations. We may also disclose health information to funeral directors so that they may carry out their duties. We may disclose personal health information to organizations that handle donations or organs, eyes or tissue and transplantations. For example, if you are an organ donor, we can release records to an organ donation facility.

Research. We may disclose your health information to researchers only if certain established measures are taken to protect your privacy. For example, we may disclose to a teaching university to conduct medical research.

To prevent a serious threat to health or safety. We may disclose your health information to the extent necessary to avoid a serious and imminent threat to your health or safety or to the health or safety of others.

Military activity and national security. We may disclose your health information to armed forces personnel under certain circumstances, and to authorized federal officials for national security and intelligence activities.

Correctional institutions. If you are an inmate, we may disclose your health information to your correctional facility to help provide you health care or to provide safety to you or others.

Workers' compensation. We may disclose your health information as required by workers' compensation laws.

Others. Unless you notify us in writing, we may disclose certain billing information to a family member calling on your behalf, such as claim status, amount paid and payment date. We will not, however, disclose medical information to them.

Your authorization

Any uses and disclosures not described in this notice will require your written authorization. Keep in mind that you may cancel your authorization at any time.

Your rights

Your right to request restrictions. You have the right to request restrictions on the way we handle your personal health information for treatment, payment or health care operations as described in the "Permitted handling of health information" section of this notice. The law, however, does not require us to agree to these restrictions. If we do agree to a restriction, we will send you written confirmation and will not use or disclose your health information in violation of that restriction. If we don't agree, we will notify you in writing.

Your right to confidential communications. We will make every effort to accommodate reasonable requests to communicate with you about your health information at an alternative location. For our records, we need your request in writing. It is important that you understand that any payment or payment information may be sent to the original address in our records.

Your right to access. You have the right to receive, by written request, a copy of your personal health information with some specified exceptions. For example, if your doctor determines that your records are sensitive, we may not give you access to your records.

Your right to amend your health information. You have the right to ask us to amend any personal health information pertaining to enrollment, payment, claims adjudication and claims or medical management records. For our records, your request for an amendment must be in writing. SCHA will not amend records in

the following situations:

- SCHA does not have the records you want amended
- SCHA did not create the records that you want amended
- SCHA has determined that the records are accurate and complete
- The records have been compiled in anticipation of a civil, criminal or administrative action or proceeding
- The records are covered by the federal Clinical Laboratory Improvement Act.

If you have requested an amendment under any of these situations, we will notify you in writing that we are denying your request. You have the right to file a written statement of disagreement with us, and we have the right to rebut that statement. Please note that changes of addresses are not required to be in writing.

Your right to information about certain disclosures

You have the right to request (in writing) information about the times we have disclosed your personal health

information for any purpose other than the following exceptions:

- Disclosures that you or your personal representative have authorized
- Certain other disclosures, such as those for national security purposes

The requirement that we provide you with information about the times we have disclosed your personal health information applies for six years from the date of the disclosure and applies only to disclosures made after April 14, 2003.

Future changes

Although SCHA follows the privacy practices described in this notice, you should know that under certain circumstances these practices could change in the future. For example, if privacy laws change, we will change our practices to comply with the law. Should this occur, we will send you a new notice prior to making a significant change in our privacy practices. The changes will then apply to all personal information we have in our possession, including any information created or received before we change the notice.

Questions and Answers

Q. Will you give my personal health information to my family or others?

A. We will only share your personal health information with others if either (1) you are present, in person or on the telephone, and give us permission to talk to the other person, or (2) you sign an authorization form.

Q. Who should I contact to get more information or get an additional copy of this notice?

A. For additional information, questions about this Notice of Privacy Practices, or if you want another copy, please visit the SCHA website at mnscha.org. You may also call or write us at the number or address listed on the back of your member ID card with questions or to obtain forms.

Q. What should I do if I believe my privacy rights have been violated?

A. If you believe SCHA has violated your privacy rights you can do the following:

- Call Member Services at the phone number on the back of your ID card.
- File a grievance with SCHA. You can call Member Services at the phone number on the back of your ID card for more information on how to do this.
- Contact the Minnesota Department of Human Services or the Office of Civil Rights at:

Minnesota Department of Human Services

Privacy Official
P.O. Box 64998
St. Paul, MN 55164-0998

Phone: (651) 431-4930 (voice)
1-800-627-3529 (TTY/TDD)
Fax: (651) 431-7441

Office of Civil Rights

Medical Privacy, Complaints Division
U.S. Department of Health & Human Services
233 N. Michigan Ave. Suite 240
Chicago, IL 60601

Phone: (312) 886-2359 (voice)
(312) 353-5693 (TTY/TDD)
Fax: (312) 886-1807

SCHA will not treat you differently if you file a complaint or grievance. More information about privacy can also be found on the U.S. Department of Health & Human Services website: <http://www.hhs.gov/ocr/privacy/>