

NO. 15-000593-CV-272

**BEVERLY T. PETERS,
individually and on behalf of all others
similarly situated,**

PLAINTIFF

v.

**ST. JOSEPH SERVICES CORP. d/b/a ST.
JOSEPH HEALTH SYSTEM and
ST. JOSEPH REGIONAL HEALTH
CENTER,**

DEFENDANTS

IN THE DISTRICT COURT

272nd JUDICIAL DISTRICT

BRAZOS COUNTY, TEXAS

PLAINTIFF'S FIRST AMENDED CLASS ACTION PETITION

Plaintiff Beverly T. Peters ("Peters" or "Plaintiff"), on behalf of herself and all others similarly situated, brings this action against Defendants St. Joseph Services Corporation d/b/a St. Joseph Health System and St. Joseph Regional Health Center (together, "St. Joseph" or "Defendants"), and respectfully shows the following:

NATURE OF THE CASE

1. This Texas data breach consumer class action seeks redress for St. Joseph's unauthorized release and disclosure of Plaintiff's and Class Members' personally identifiable information ("PII") and confidential, privileged, and protected health information ("PHI") (together, "PII/PHI"). Plaintiff brings this action on behalf of several hundred thousand similarly situated Texas citizens (*i.e.*, the Class Members) who entrusted their PII/PHI to St. Joseph in connection with purchasing health care services, including PII/PHI protection services, from St. Joseph based on St. Joseph's assurances that (i) the proper data security measures, policies, procedures, controls, protocols, and software and hardware systems were in

place and operational to safeguard and protect their PII/PHI, and (ii) St. Joseph would not release or disclose their PII/PHI without authorization.

2. St. Joseph, however, willfully, intentionally, recklessly and/or negligently failed to safeguard and protect Plaintiff's and Class Members' PII/PHI, which resulted in its unauthorized release and disclosure to fraudsters over several days by its inadequately protected computer system that was specifically targeted by the fraudsters (the "Data Breach"). On information and belief, Plaintiff's and Class Members' wrongfully released and disclosed PII/PHI was unencrypted. The St. Joseph Data Breach is one of the largest data breaches involving PHI in the history of the United States.

3. Plaintiff is a former St. Joseph patient. The Class Members are current and former St. Joseph patients, employees and some employees' beneficiaries. According to St. Joseph's February 4, 2014 press release revealing the Data Breach, the wrongfully released and disclosed PII/PHI includes names, Social Security numbers, dates of birth, medical information (*i.e.*, PHI), and possibly addresses. The Data Breach also could involve other forms of Plaintiff's and Class Members' PII/PHI.

4. St. Joseph flagrantly disregarded Plaintiff's and Class Members' privacy rights by intentionally, willfully, recklessly and/or negligently failing to take the necessary precautions required to safeguard and protect their PII/PHI, thereby wrongfully releasing and disclosing their PII/PHI without authorization. Plaintiff's and Class Members' PII/PHI was improperly handled and stored by St. Joseph, inadequately secured, on information and belief, unencrypted, unprotected, readily able to be copied by data thieves, not kept in accordance with applicable, required, and appropriate cyber-security measures, policies, procedures, controls, and/or protocols, and wrongfully disclosed. As described in greater detail below, the wrongfully

disclosed and compromised PII/PHI was transferred, sold, opened, read, mined and otherwise used without Plaintiff's and Class Members' authorization, thereby causing them to suffer economic damages and other actual injury and harm.

5. St. Joseph's wrongful actions, inaction and/or omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiff's and Class Members' PII/PHI violated the (i) Texas Medical Practice Act, TEX. OCC. CODE §159.001, *et seq.*, (ii) Texas Hospital Licensing Law, TEX. HEALTH & SAFETY CODE §241.001, *et seq.*, and (iii) Texas Deceptive Trade Practices-Consumer Protection Act, TEX. BUS. & COM. CODE §17.41, *et seq.*

6. St. Joseph's wrongful actions, inaction and/or omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiff's and Class Members' PII/PHI also constitute negligence/gross negligence, negligence *per se*, breach of contract, breach of implied contract, invasion of privacy, breach of fiduciary duty, breach of confidentiality, and money had and received/assumpsit under Texas common law.

7. Plaintiff, on behalf of herself and Class Members, seeks, *inter alia*, actual damages, consequential damages, nominal damages, exemplary damages, treble damages, injunctive relief, attorneys' fees, litigation expenses and/or costs of suit.

8. Pursuant to the Texas Medical Practice Act, TEX. OCC. CODE §159.009(a), and the Texas Hospital Licensing Law, TEX. HEALTH & SAFETY CODE §241.156(c), Plaintiff's request for injunctive relief takes precedence over all civil matters on the Court's docket except those matters to which equal precedence on the docket is granted by law.

DISCOVERY PLAN

9. Plaintiff, on behalf of herself and Class Members, intends to seek entry of a Level 3 order requiring discovery to be conducted in accordance with a discovery control plan tailored to the specific circumstances of this action. TEX. R. CIV. P. 190.4.

PARTIES

10. Plaintiff is a citizen and resident of Brenham, Texas. Peters is a former St. Joseph patient who, at all relevant times, purchased health care services, including PII/PHI protection services, from St. Joseph and its affiliated physicians at several of its health care facilities in Texas. Peters entrusted her PII/PHI to St. Joseph in connection with purchasing such services based on St. Joseph's assurances that the proper data security measures, policies, procedures, controls, protocols, and software and hardware systems were in place and operational to safeguard and protect her PII/PHI, and St. Joseph would not release or disclose her PII/PHI without authorization. Peters' PII/PHI, however, was wrongfully released and disclosed without her authorization in the Data Breach—as confirmed by the February 4, 2014 Data Breach notification letter she received from St. Joseph. *See* Exhibit A.

11. Peters has never been victimized by a data breach other than the St. Joseph Data Breach. She meticulously protects her PII/PHI. She utilizes different passwords for each of her online financial, credit card, and retail accounts, changing them on a regular basis. She closely monitors her bank account, regularly checking it online at least every other day for irregular activity. She also maintains her hard copy credit card and financial account statements in a safe for five years, after which she personally burns them in a trash barrel on her property.

12. As a direct and/or proximate result of St. Joseph's wrongful actions, inaction and/or omissions and the resulting Data Breach, Peters' PII/PHI was wrongfully released and

disclosed without authorization to unauthorized third parties in the public domain who have since inflicted identity theft and/or identity fraud on her in the form of, *inter alia*, attempted unauthorized charges on her Discover card. Peters was required by St. Joseph to provide (and provided) her Discover card account number to St. Joseph on forms she submitted to St. Joseph in connection with purchasing health care and PII/PHI protection services. After the Data Breach, and while she was in Texas, Peters received a text from Discover requesting approval of an unauthorized, out of the ordinary retail purchase in Pennsylvania. When Peters declined to approve the purchase, Discover immediately closed her account, and reissued a new payment card to her. Prior to the Data Breach, Peters never experienced any attempt by fraudsters to access her Discover card account.

13. As a direct and/or proximate result of St. Joseph's wrongful actions, inaction and/or omissions, the resulting Data Breach, and its unauthorized release and disclosure of her PII/PHI, Peters also suffered actual identity theft and/or identity fraud in the form of the breach of her Yahoo email account which, along with her Social Security number and Texas Driver's License number, also were required by St. Joseph to be submitted (and were submitted) in connection with purchasing health care services. All of Peters' online financial, credit card, and retail accounts are linked to her Yahoo email account. After the Data Breach, friends and relatives reported receiving large volumes of spam email from her Yahoo email account that they had never received before. As a result, Peters spent time changing the password on her Yahoo email account. Prior to the Data Breach, Peters never experienced any attempt by fraudsters to access her Yahoo email account and/or her online financial, credit card, and retail accounts.

14. As a direct and/or proximate result of St. Joseph's wrongful actions, inaction and/or omissions, the resulting Data Breach, and its unauthorized release and disclosure of her

PII/PHI, Peters also suffered actual identity theft and/or identity fraud in the form of the unauthorized access of her Amazon.com account by an unidentified fraudster. The fraudster attempted to access her Amazon.com account using her son's name, which only could have been obtained from her wrongfully disclosed and compromised PHI wherein St. Joseph required her to provide the names and contact information of her next of kin (which she provided in connection with purchasing health care services). Peters spent time investigating the attempted unauthorized access of her Amazon.com account, confirming that her son did not attempt to access the account. Prior to the Data Breach, Peters never experienced any attempt by fraudsters to access her Amazon.com account.

15. As a direct and/or proximate result of St. Joseph's wrongful actions, inaction and/or omissions, the resulting Data Breach, and its unauthorized release and disclosure of her PII/PHI, Peters also suffered actual identity theft, identity fraud and/or medical fraud in the form of multiple telephone solicitations from medical products and services companies asking to speak with specific members of her family. This information only could have been obtained from her wrongfully released, disclosed, and compromised PHI wherein St. Joseph required her to provide the names and contact information of her next of kin (which she provided in connection with purchasing health care services). On the average, Peters deals with 2-3 such calls a day at all times of the day and night. Prior to the Data Breach, Peters never received such telephone solicitations.

16. As a direct and/or proximate result of St. Joseph's wrongful actions, inaction and/or omissions, the resulting Data Breach, and its unauthorized release and disclosure of her PII/PHI, Peters also suffered actual identity theft, identity fraud and/or medical fraud in the form of unsolicited emailed and mailed marketing materials specifically targeting confidential medical

conditions detailed in her wrongfully disclosed PII/PHI that the senders only could have learned about from her wrongfully disclosed PII/PHI. Prior to the Data Breach, Peters never received such targeted marketing materials.

17. As a direct and/or proximate result of St. Joseph's wrongful actions, inaction and/or omissions, the resulting Data Breach, and the resulting actual identity theft, identity fraud and/or medical fraud inflicted on her by one or more unauthorized third parties, Peters has suffered (and will continue to suffer) economic damages and other actual harm in the form of the deprivation of the full value of her PII/PHI, for which there are well-established national and international markets. PII/PHI is a unique and valuable property right.¹ Moreover, once PII/PHI is out, it is gone. The fundamental economic principle of supply and demand supports the fact that since Peters' PII/PHI is now available on the open market, she would receive far less for it

¹ See, e.g., John T. Soma, *et al*, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3-*4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

The unauthorized release and disclosure of PHI is also gravely serious; to wit, a fraudster is able to use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII/PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully released and disclosed PHI to adjust their insureds' medical insurance premiums.

The value of PHI as a commodity also is measurable. See, e.g., Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for \$50 Each on Black Market* (April 28, 2014), <http://www.medscape.com/viewarticle/824192> (last visited June 26, 2014); Adam Greenberg, *Health Insurance Credentials Fetch High Prices in the Online Black Market* (July 16, 2013) (all-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, Social Security numbers and bank account information, complete with account and routing numbers, are fetching \$1,200 to \$1,300 each), <http://www.scmagazine.com/health-insurance-credentials-fetch-high-prices-in-the-online-black-market/article/303302/> (last visited June 26, 2014).

now if she attempted to sell her PII/PHI—which she is able to do—than had the PII/PHI not already been wrongfully released and disclosed by St. Joseph. Faced with the choice of having her PII/PHI wrongfully released, disclosed, compromised, transferred, sold, opened, read, mined and otherwise used without her authorization versus selling her PII/PHI and receiving the compensation herself, Peters would choose the latter.² Peters—not fraudsters—should have the exclusive right to monetize her PII/PHI at the highest possible value. St. Joseph’s wrongful actions, inaction and/or omissions and the resulting Data Breach deprived her of the full value of this unique property right.

18. As a direct and/or proximate result of St. Joseph’s wrongful actions, inaction and/or omissions, the resulting Data Breach, and the resulting actual identity theft, identity fraud and/or medical fraud inflicted on her by one or more unauthorized third parties, Peters has suffered (and will continue to suffer) economic damages and other actual injury and harm, including, *inter alia*, (i) invasion of privacy, (ii) breach of the confidentiality of her PII/PHI, (iii) lost benefit of her bargain, (iv) diminished value of the services she purchased from St. Joseph,

² It also is important to note that in the case of identity theft or identity fraud, after a victim goes through the hassle of closing credit cards, changing passwords on financial accounts, and notifying lenders and the credit bureaus, the victim’s PII is again private from that point forward.

In the case of medical data breach, however, there is no opportunity for a clean start. Once a victim’s PHI is out—such as Peters’ and Class Members’ PHI—it is out forever. Any negative stigma associated with a victim’s PHI—such as a sexually-transmitted disease, an abortion, a sex change operation or a slow-growing cancer—cannot be undone.

Even worse, the consequences of having one’s PHI fall into the hands of unscrupulous individuals can literally be life threatening. When a fraudster uses a victim’s PHI to obtain medical care, the imposter’s information ends up on the victim’s medical record. If the victim of a wrongful PHI disclosure subsequently was involved in an accident and rushed to the emergency room, doctors utilizing his or her PHI would see the wrong blood type, not know the victim is allergic to certain medications, and/or has a pre-existing condition—which, in turn, could lead to misdiagnosis or mistreatment with potentially deadly consequences.

and (v) the certainly impending and/or increased substantial risk of future economic damages and other actual injury and harm.

19. Defendant St. Joseph Services Corporation d/b/a St. Joseph Health System (“SJSC”) is a Texas corporation with its principal place of business in Bryan, Texas. SJSC is a Texas health system with facilities in eight Texas counties, including Brazos County, serving more than 325,000 residents. SJSC has five hospitals, two long term care centers, and over a dozen physician clinic locations. SJSC’s wrongful actions, inaction and/or omissions form a significant basis of Plaintiff’s claims. Plaintiff, therefore, on behalf of herself and Class Members, seeks significant relief from SJSC. SJSC may be served with Citation and a copy of this First Amended Class Action Petition by serving its registered agent for service of process, C.T. Corporation System, 1999 Bryan Street, Dallas, TX 75201-3140.

20. Defendant St. Joseph Regional Health Center (“SJRHC”) is a Texas corporation with its principal place of business in Bryan, Texas. SJRHC owns and operates a 310-bed regional health care center in Bryan, Texas, as well as several other St. Joseph-branded health care facilities in Texas. Plaintiff purchased and received health care services from at least two of these St. Joseph facilities (and possibly also from SJSC). SJRHC’s wrongful actions, inaction and/or omissions form a significant basis of Plaintiff’s claims. Plaintiff, therefore, on behalf of herself and Class Members, seeks significant relief from SJRHC. SJRHC may be served with Citation and a copy of this First Amended Class Action Petition by serving its registered agent for service of process, C.T. Corporation System, 1999 Bryan Street, Dallas, TX 75201-3140.

21. SJSC and SJRHC together will be referred to as “St. Joseph.”

JURISDICTION AND VENUE

22. This Court has subject matter jurisdiction over Plaintiff's claims because the amount in controversy is within the Court's jurisdictional limits. TEX. R. CIV. P. 47(b). Plaintiff, on behalf of herself and Class Members, seeks monetary relief of over \$1,000,000 (one million dollars). TEX. R. CIV. P. 47(c)(5). This Court has personal jurisdiction over St. Joseph because at all relevant times, all of the events giving rise to this action occurred in Brazos County, Texas—*i.e.*, St. Joseph's wrongful actions, inaction and/or omissions that caused the unauthorized release and disclosure of Plaintiff's and Class Members' PII/PHI via the breach of its server located in Brazos County, Texas—and St. Joseph resides, is located, can be found, and conducts substantial business in Brazos County, Texas (and continues to do so).

23. Venue is proper in Brazos County, Texas, pursuant to TEX. CIV. & PRAC. CODE §15.002(a)(1); (a)(3) because at all relevant times, (i) all of St. Joseph's wrongful actions, inaction and/or omissions giving rise to this action occurred in Brazos County, Texas, (ii) St. Joseph resides, can be found, and conducts substantial business in Brazos County, Texas (and continues to do so), and (iii) St. Joseph's principal office is located in Brazos County, Texas.

FACTS

I. Data breaches directly lead to identity theft, identity fraud, medical fraud, and multiple forms of economic damages and other actual injury and harm.

24. According to the United States Government Accountability Office (GAO), the terms "identity theft" or "identity fraud" are broad terms encompassing various types of criminal activities, such as credit card fraud, telephone or utilities fraud, bank fraud and government fraud (*i.e.*, theft of government services). Identity theft occurs when a person's PII/PHI is used

without authorization to commit fraud or other crimes. *See* Federal Trade Commission (FTC), *Fighting Back Against Identity Theft*.³

25. Also according to the FTC, “the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and that any privacy framework should recognize additional harms that might arise from unanticipated uses of data.”⁴ Furthermore, “there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII.”⁵

26. Moreover, “[o]nce identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance. An identity thief can file a tax refund in your name and get your refund.”⁶

27. Medical fraud (also known as medical identity theft) occurs when a person’s personal information is used without authorization to obtain, or receive payment for, medical treatment, services or goods.⁷ For example, as of 2010, more than 50 million people in the

³ <http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html> (last visited March 7, 2015).

⁴ Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change* (March 2012).

⁵ Federal Trade Commission, *A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, (Dec. 2010), <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf> (last visited March 7, 2015).

⁶ Federal Trade Commission, *Signs of Identity Theft*, <http://www.consumer.ftc.gov/articles/0271-signs-identity-theft> (last visited March 7, 2015).

⁷ *See* www.ftc.gov/bcp/edu/microsites/idtheft/consumers/resolving-specific-id-theft-problems.html (last visited March 24, 2014).

United States did not have health insurance according to the U.S. census. This, in turn has led to a surge in medical identity theft as a means of fraudulently obtaining medical care.

28. A fraudster can easily secure the email address of a data breach victim. When a fraudster has access to PII/PHI from a large group of similarly situated victims, it is much more feasible to develop a believable phishing⁸ spoof email that appears realistic. The fraudster can then convince the group of victims to reveal additional confidential PII/PHI.

29. The GAO found that identity thieves use PII/PHI to open financial and payment card accounts, running up charges in a victim's name. This type of identity theft is the "most damaging" because it may take a while for the victim to become aware of the theft. In the meantime, the identity theft and identity fraud causes significant harm to the victim's credit rating and finances. Moreover, unlike other PII/PHI, Social Security numbers are incredibly difficult to change and their misuse generally continues for years into the future.

30. Identity thieves also use Social Security numbers to commit other types of fraud, such as obtaining false identification cards, obtaining government benefits in the victim's name, committing crimes and/or filing fraudulent tax returns on the victim's behalf to obtain fraudulent tax refunds. Identity thieves also obtain jobs using compromised Social Security numbers, rent houses and apartments and/or obtain medical services in the victim's name. The GAO also found victims of identity theft face "substantial costs and inconvenience repairing damage to their credit records" and the damage to their "good name." *Id.*

⁸ "Phishing" is an attempt to acquire information (and sometimes, indirectly, money), such as usernames, passwords and credit card details by masquerading as a trustworthy entity through an electronic communication. Communications purporting to be from popular social websites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public. Phishing emails typically contain links to websites infected with malware. Phishing is carried out by e-mail spoofing or instant messaging, often directing users to enter details at a fake copycat website that looks and feels almost identical to the legitimate one.

31. The unauthorized disclosure of a person's Social Security number is particularly harmful since Social Security numbers cannot be easily replaced like a credit card or debit card, and it takes a substantial amount of time to do so. In order to obtain a new Social Security number, a person must show evidence that someone used the number fraudulently and the victim has been disadvantaged by the misuse.⁹ Thus, a victim of the wrongful disclosure of PII/PHI cannot obtain a new Social Security number until the damage has already been done.

32. Obtaining a new Social Security number also is not an absolute prevention against identity theft and identity fraud. Government agencies, private businesses and credit reporting companies typically still have a victim's records under the old number, so using a new number will not guarantee a fresh start. For some victims of identity theft and identity fraud, a new Social Security number will actually create new problems. Because prior positive credit information is not associated with the new Social Security number, it will be more difficult to obtain credit due to the absence of a credit history. Thus, data breaches directly lead to identity theft, identity fraud and/or medical fraud, and multiple forms of economic damages and other actual injury and harm.

II. The Privacy Notice—St. Joseph's Contractual Privacy Obligations to Plaintiff and Class Members.

33. As a condition to providing health care services, St. Joseph requires its patients to provide their detailed PII/PHI. Indeed, St. Joseph recognizes that maintaining the confidentiality of its patients' PII/PHI is critical and contractual as a matter of law:

St. Joseph is required by law to maintain the privacy of health information about you that can identify you ("Protected Health Information" or "PHI"), to provide

⁹ See *Identity Theft and Your Social Security Number*, SSA Publication No. 05-10064 (October 2007).

you with this Notice of our legal duties and privacy practices with respect to your PHI, and to abide by the terms of the Notice currently in effect.

See St. Joseph Privacy Notice in effect at the date of the Data Breach (Exhibit B) at 1.

Moreover:

Safeguarding patients' health information is *not only a legal requirement but also an important ethical obligation*. As a health care provider, St. Joseph and its staff are entrusted with clinical information regarding our patients. *We recognize that medical and billing records are highly confidential and must be treated with great respect and care* by all staff with access to this information. St. Joseph's policy regarding confidentiality of protected health care information reflects *our strong commitment to protecting the confidentiality of our patients' medical records and clinical information*.

(emphasis added). See St. Joseph Notice of Privacy Policies, <http://www.st-joseph.org/body.cfm?id=461> (last visited March 7, 2015).

34. St. Joseph makes certain representations, warranties and commitments to its patients regarding the privacy of their PII/PHI in its Privacy Notice (Exhibit B). The Privacy Notice is posted in each St. Joseph facility (*id.* at 1) and on the St. Joseph website.¹⁰ The Privacy Notice is also given to every St. Joseph patient—including Plaintiff and Class Members. Indeed, each St. Joseph patient must sign the Privacy Notice, acknowledging its existence and terms as a condition to receiving health care services. *Id.* at 3. Plaintiff signed the Privacy Notice.

35. St. Joseph itemizes its privacy obligations to its patients in the Privacy Notice, making a firm commitment to uphold them:

We understand that all information about you and your health is personal. We are committed to protecting this information. When you receive services at a St. Joseph Facility/Entity, a medical record is created. This record describes the services provided to you and is needed to provide you with quality care and to comply with certain legal requirements. This Notice applies to records of your care generated by St. Joseph, whether made by a St. Joseph employee or a physician involved in your care.

¹⁰ See <http://www.st-joseph.org/workfiles/privacy.pdf> (last visited March 7, 2015).

Privacy Notice (Exhibit B) at 1 (emphasis added).

36. The Privacy Notice lists the following specific and limited permissible purposes for which St. Joseph may use and disclose all or a portion of its patients' PII/PHI without their authorization:

- (i) Treatment, payment and health care operations;
- (ii) Sharing with other organizations in connection with treatment, payment and health care operations;
- (iii) Inclusion in a specific St. Joseph facility patient directory;
- (iv) Disclosure to relatives and close friends to the extent necessary to assist with a patient's health care or to secure payment for the patient's health care;
- (v) Disclosure for purpose of assisting disaster relief efforts;
- (vi) Medical research in limited situations;
- (vii) Fundraising activities; and
- (viii) Disclosures required by law, such as pertaining to various listed public health activities.

Id. at 1-2.

37. *"For any purpose other than the ones described above, your PHI may be used or disclosed only when you provide your written authorization on an approved authorization form."*

Privacy Notice at 2 (emphasis added). In other words, St. Joseph commits that *"for any purpose other than the ones described above,"* a patient's PII/PHI will not be disclosed without authorization. *Id.* There are no exceptions.

38. Regarding its patients' rights pertaining to their PHI, St. Joseph further represents and promises that "[i]n certain [undefined] instances, you have the right to be notified in the event that we, or one of our Business Associates, discover an inappropriate use or disclosure of

your health information. Notice of any such use or disclosure will be made in accordance with state and federal requirements.” Privacy Notice (Exhibit B) at 3.

39. St. Joseph further represents and promises its patients that they also “have the right to request an ‘accounting of disclosures.’ This is a list of disclosures that we have made about you.” *Id.*

40. Finally, regarding the PII/PHI entrusted to it, St. Joseph represents and promises that it “safeguards customer information using various tools such as firewalls, passwords and data encryption” and “continually strive[s] to improve these tools to meet or exceed industry standards.” *Id.* Ironically, St. Joseph also promises to “limit access to [its patients’] information to protect against its unauthorized use.” *Id.* St. Joseph’s data security efforts, however, unfortunately failed across the board.

III. The St. Joseph Data Breach.

41. On February 4, 2014, St. Joseph announced to the public, for the first time, that at least between December 16, 2013 and December 18, 2013, an unprotected server on its computer system located in Brazos County, Texas, storing confidential and privileged patient and employee files for several St. Joseph facilities (*i.e.*, the PII/PHI) wrongfully granted unauthorized access to parties operating from IP addresses in China and elsewhere, thereby releasing and disclosing Plaintiff’s and Class Members’ PII/PHI to the fraudsters without authorization. The fraudsters deliberately targeted the St. Joseph server because it was not properly protected.

42. The breached server contained the PII/PHI of Plaintiff and approximately 405,000 Class Members, including their names, Social Security numbers, birthdates, addresses, medical information, and bank account information. The fraudsters spent at least three days (and possibly longer) collecting Plaintiff’s and Class Members’ PII/PHI. Other confidential PII or

PHI information may also have been wrongfully disclosed. On information and belief, none of the wrongfully released, disclosed, and compromised PII/PHI was encrypted.

43. St. Joseph also announced it was belatedly “taking appropriate additional security measures to strengthen the security of its system,” (*id.*), which are the PII/PHI data security measures, policies, procedures, controls, protocols, and software and hardware systems it should already have instituted. Had such PII/PHI data security measures, policies, procedures, controls, protocols, and software and hardware systems been in place, functioning and properly monitored, the Data Breach never would have occurred. On information and belief, at the time of the Data Breach, St. Joseph was not compliant with the Texas Medical Records Privacy Act, Texas Medical Practice Act, Texas Hospital Licensing Law, Section 521.052 of the Texas Business and Commerce Code, and/or the industry standards St. Joseph references in its Privacy Notice that it claims to “meet or exceed.” *See* Privacy Notice (Exhibit B) at 3.

44. What’s more, despite knowing about the Data Breach since at least December 18, 2013, St. Joseph did not announce the Data Breach and/or commence sending Data Breach notification letters to Plaintiff and Class Members until February 4, 2014—almost seven weeks later. St. Joseph’s failure to timely notify Plaintiff and Class members about the Data Breach notification violated Section 521.053 of the Texas Business and Commerce Code. Had Plaintiff and Class Members known about the Data Breach sooner, they could have taken certain defensive measures much earlier—such as, without limitation, changing financial account and payment card passwords and email addresses—to mitigate their injuries, harm, and damages. In addition to the Data Breach itself, St. Joseph’s post-Data Breach notification delay further exacerbated the situation, substantially increasing the risk of future economic damages and other actual injury and harm to Plaintiff and Class Members.

45. During the intervening period between the Data Breach and the date the Data Breach notification letters were sent to Plaintiff and Class Members, their unencrypted PII/PHI, on information and belief, was transferred, sold, opened, read, mined and otherwise used without their authorization—as evidenced by the identity theft, identity fraud and/or medical fraud Plaintiff has already suffered—while they had no chance whatsoever to take measures to protect its confidentiality, their credit, and/or their finances.

46. Rather than getting out in front of the Data Breach and proactively offering Plaintiff and Class Members real protection from identity theft, identity fraud and/or medical fraud resulting from their wrongfully disclosed and compromised PII/PHI, St. Joseph only offered them one year of credit monitoring (Exhibit A)—even though it is well known that fraudsters routinely use compromised PII/PHI for longer than a year. Even then, only a year of credit monitoring is woefully insufficient given the trove of unencrypted PII/PHI wrongfully released and disclosed to the world in the Data Breach by St. Joseph, and the manipulation and machinations of fraudsters and cyber criminals.

47. In truth, the actual post-Data Breach “PII/PHI protection services” allegedly offered by St. Joseph and at what price are remarkably indiscernible—which could be a violation of the Texas Deceptive Trade Practices-Consumer Protection Act in itself. At best, the proffered credit monitoring indirectly tracks identity theft; while it may reveal new credit accounts opened with the wrongfully disclosed information, it will do nothing to monitor unauthorized charges made to, for example, existing payment card accounts. After data breach victims enroll in this type of program, program vendors and the credit reporting agencies typically treat their enrollment as golden opportunities to push other unnecessary products and services—thereby further damaging data breach victims.

48. Notwithstanding St. Joseph's promises, the offered "PII/PHI protection services," in truth, are significantly less than advertised. In the fine print in its Terms of Use attached to the Data Breach notification letters (Exhibit A), AllClear ID, the credit monitoring program vendor, states it (i) "will not make payments or reimbursements to you for any loss or liability you may incur," and (ii) "does not promise to help you improve your credit history or rating beyond resolving incidents of fraud." As a further condition of receiving AllClear ID "protection services," Plaintiff and Class Members must not fall victim to phishing emails and disclose their PII—which could easily result from the Data Breach. In other words, if a Class Member is victimized by a phishing scam fueled by the PII/PHI disclosed by St. Joseph in the Data Breach, he or she will lose the AllClear ID "protection services" offered as a result of the Data Breach.

49. St. Joseph's Data Breach notification letters also shift the burden and expense of the Data Breach to Plaintiff and Class Members by, *inter alia*, advising them to incur the time and expense to (i) regularly purchase their credit reports from the three major credit reporting agencies, (ii) contact the agencies, law enforcement, state attorney general and/or the FTC if anything in their financial or retail accounts look amiss, (iii) place fraud alerts on their credit reports, and (iv) place and/or lift freezes on their credit files, which must be instituted at each credit reporting agency (*i.e.*, Equifax, Experian, and TransUnion) at a cost of \$5 to \$20 an action. All of these actions will take time and money to effectuate—which St. Joseph encouraged Plaintiff and Class Members to incur, but has not offered to pay.

IV. The St. Joseph Data Breach Inflicted Economic Damages and Other Actual Injury and Harm on Plaintiff and Class Members.

50. St. Joseph's above-described wrongful actions, inaction and/or omissions—to wit, failing to protect Plaintiff's and Class Members' PII/PHI with which it was entrusted—directly and/or proximately caused the Data Breach, and the wrongful release and disclosure of Plaintiff's

and Class Members' unencrypted PII/PHI into the public domain without their knowledge, authorization, and/or consent.

51. St. Joseph flagrantly and/or negligently disregarded and/or violated Plaintiff's and Class Members' privacy rights, and harmed them in the process, by not obtaining their prior written authorization and consent to disclose their PII/PHI to any other person or organization and/or for any purpose other than the persons, organizations and purposes listed in the Privacy Notice—as required by, *inter alia*, the Privacy Notice, the Texas Medical Records Privacy Act, the Texas Medical Practice Act, the Texas Hospital Licensing Law, Section 521.052 of the Texas Business and Commerce Code, and/or the industry standards referenced in its Privacy Notice that St. Joseph claims to “meet or exceed.” *See* Exhibit B at 3.

52. St. Joseph flagrantly and/or negligently disregarded and/or violated Plaintiff's and Class Members' privacy rights, and harmed them in the process, by failing to identify, implement, maintain and/or monitor appropriate data security measures, policies, procedures, controls, protocols, and software and hardware systems to ensure the security and confidentiality of Plaintiff's and Class Members' PII/PHI, and wrongfully releasing and disclosing their PII/PHI without authorization. St. Joseph's unwillingness or inability to identify, implement, maintain and/or monitor such data security measures, policies procedures, controls, protocols, and software and hardware system—while, at the same time, claiming in its Privacy Notice that such “tools” were in place (*id.* at 3)—is an abuse of discretion, false, and misleading, confirming St. Joseph's intentional and willful conduct.

53. St. Joseph's untimely and inadequate Data Breach notification—including its failure to provide Plaintiff and Class Members with any meaningful protection or relief from the Data Breach—is misleading and, even worse, substantially increases Plaintiff's and Class

Members' risk of future economic damages and other actual harm resulting from identity theft, identity fraud and/or medical fraud.

54. St. Joseph's above-described wrongful actions, inaction and/or omissions—to wit, St. Joseph's failure to identify, implement, maintain and monitor the proper data security measures, policies, procedures, controls, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class Members' PII/PHI—directly and/or proximately caused the Data Breach, caused the unauthorized release and disclosure of Plaintiff's and Class Members' PII/PHI, and caused Plaintiff and Class Members to suffer economic damages and other actual injury and harm. Had St. Joseph not engaged in such wrongful actions, inaction and/or omissions, the Data Breach never would have occurred and Plaintiff's and Class Members' PII/PHI would not have been wrongfully released, disclosed, compromised, disseminated to the world, and wrongfully used. Plaintiff and Class Members, therefore, are entitled to injunctive relief and/or compensation for their economic damages and other actual harm, including, *inter alia*, (i) actual identity theft, identity fraud and/or medical fraud, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI, (iv) lost benefit of their bargains, (v) deprivation of the full value of their PII/PHI, for which there are well-established national and international markets, (vi) diminished value of the medical services they purchased from St. Joseph, and (vii) the certainly impending and/or increased substantial risk of future economic damages and other actual injury and harm.

CLASS ACTION ALLEGATIONS

55. Pursuant to TEX. R. CIV. P. 42, Plaintiff brings this action as a class action on behalf of herself and the following Class of similarly situated individuals:

All Texas citizens whose personally identifiable information and/or protected health information (PII/PHI) was maintained on a St. Joseph computer system server that was breached between December 16, 2013 and December 18, 2013, inclusive, and released and disclosed without authorization.

Excluded from the Class are (i) St. Joseph officers, directors, senior management, and any St. Joseph officer, director, employee, representative, or agent who knew the breached server was not properly protected prior to the Data Breach, and (ii) the Court and Court personnel.

56. The Class Members are so numerous that their joinder is impracticable. According to information provided by St. Joseph, there are several hundred thousand Class Members. More than two-thirds (*i.e.*, 100%) of the members of the proposed class are Texas citizens. The precise identities of the Class Members and their addresses are currently unknown to Plaintiff, but can be easily derived from St. Joseph's internal records that were used to send the Data Breach notification letters to Plaintiff and Class Members in February 2014.

57. St. Joseph's above-described wrongful actions, inaction and/or omissions that caused the Data Breach and the unauthorized release and disclosure of Plaintiff's and Class Members' PII/PHI violated their rights in a virtually identical manner.

58. Questions of law and fact common to all Class Members predominate over any questions affecting only individual Class Members including, *inter alia*:

- (i) Whether St. Joseph's wrongful release and disclosure of Plaintiff's and Class Members' PII/PHI without authorization violated the Texas Medical Practice Act;
- (ii) Whether St. Joseph's wrongful release and disclosure of Plaintiff's and Class Members' PII/PHI without authorization violated the Texas Hospital Licensing Law;

- (iii) Whether St. Joseph's wrongful release and disclosure of Plaintiff's and Class Members' PII/PHI without authorization constitutes negligence and/or gross negligence;
- (iv) Whether St. Joseph's wrongful release and disclosure of Plaintiff's and Class Members' PII/PHI without authorization constitutes negligence *per se*;
- (v) Whether St. Joseph's wrongful release and disclosure of Plaintiff's and Class Members' PII/PHI without authorization constitutes breach of contract;
- (vi) Whether St. Joseph's wrongful release and disclosure of Plaintiff's and Class Members' PII/PHI without authorization constitutes breach of implied contract;
- (vii) Whether St. Joseph's wrongful release and disclosure of Plaintiff's and Class Members' PII/PHI without authorization violated the Texas Deceptive Trade Practices-Consumer Protection Act;
- (viii) Whether St. Joseph's wrongful release and disclosure of Plaintiff's and Class Members' PII/PHI without authorization constitutes invasion of privacy;
- (ix) Whether St. Joseph's wrongful release and disclosure of Plaintiff's and Class Members' PII/PHI without authorization constitutes breach of fiduciary duty;
- (x) Whether St. Joseph's wrongful release and disclosure of Plaintiff's and Class Members' PII/PHI without authorization constitutes a breach of confidentiality at Texas common law;
- (xi) Whether St. Joseph's wrongful release and disclosure of Plaintiff's and Class Members' PII/PHI without authorization invokes the equitable doctrines of money had and received/assumpsit;
- (xii) Whether Plaintiff and Class Members sustained harm and damages as a direct and/or proximate result of St. Joseph's wrongful release and disclosure of Plaintiff's and Class Members' PII/PHI without authorization and, if so, the amount of such damages;
- (xiii) Whether Plaintiff and Class Members are entitled to exemplary damages as a direct and/or proximate result of St. Joseph's wrongful release and disclosure of Plaintiff's and Class Members' PII/PHI without authorization and, if so, the amount of such damages; and
- (xiv) Whether Plaintiff and Class Members are entitled to injunctive and/or declaratory relief as a direct and/or proximate result of St. Joseph's wrongful release and disclosure of Plaintiff's and Class Members' PII/PHI without authorization.

59. Plaintiff's claims are typical of the Class Members' claims because she, like all Class Members, is a victim of St. Joseph's above-described wrongful actions, inaction and/or omissions—to wit, its failure to identify, implement, maintain and monitor the proper data security measures, policies, procedures, controls, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class Members' PII/PHI, and wrongful and unauthorized release and disclosure of their PII/PHI—that directly and/or proximately caused the Data Breach, and caused them to suffer the resulting economic damages and other actual injury and harm.

60. Plaintiff has no interests antagonistic to, or in conflict with, Class Members' interests. Plaintiff is willing and able to take an active role in controlling the litigation and protecting the absent Class Members. Plaintiff knows of no difficulties likely to be encountered in the management of this action as a class action.

61. Plaintiff and her counsel will fairly and adequately represent the Class Members' interests. Plaintiff's attorneys are highly experienced in the prosecution of consumer class actions, including data breach cases, and will vigorously prosecute this action on behalf of Plaintiff and Class Members as they have to date.

62. A class action is superior to all other available methods for fairly and efficiently adjudicating Plaintiff's and Class Members' claims. Plaintiff and Class Members have been irreparably harmed as a result of St. Joseph's wrongful actions, inaction and/or omissions and the resulting Data Breach, and the unauthorized release and disclosure of their PII/PHI. Litigating this case as a class action is appropriate because (i) it will avoid a multiplicity of suits and the corresponding burden on the courts and Parties, (ii) it would be virtually impossible for all Class Members to intervene as parties-plaintiff in this action, (iii) it will allow numerous individuals with claims too small to adjudicate on an individual basis because of prohibitive litigation costs

to obtain redress for their injuries, and (iv) it will provide Court oversight of the claims process once St. Joseph's liability is adjudicated.

63. Class certification, therefore, is appropriate under TEX. R. CIV. P. 42(b)(3) because the above common questions of law or fact predominate over any questions affecting individual Class Members, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

64. Class certification also is appropriate under TEX. R. CIV. P. 42(b)(2) because St. Joseph has acted, or refused to act, on grounds generally applicable to the Class, thereby making appropriate final injunctive relief with respect to the Class as a whole.

65. Class certification also is appropriate under TEX. R. CIV. P. 42(b)(1) because the prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications, which would establish incompatible standards of conduct for St. Joseph. For example, one court might decide the challenged actions are illegal and enjoin St. Joseph, while another court might decide the same actions are not illegal. Separate actions, as a practical matter, also could be dispositive of, impair or impede the interests of other Class Members who are not parties to such actions, and/or substantially impair or impede their ability to protect their interests.

66. Absent a class action, St. Joseph will escape liability for its wrongdoing despite its serious violations of the law, and its infliction of economic damages and other actual injury and harm on Plaintiff and Class Members.

CLAIMS FOR RELIEF/CAUSES OF ACTION

COUNT I

VIOLATION OF THE TEXAS MEDICAL PRACTICE ACT (TEX. OCC. CODE § 159.001, et seq.)

67. The previous factual statements and allegations are incorporated by reference.

68. Under TEX. OCC. CODE § 159.002(a);(b), communications between a physician and a patient, relative to, or in connection with, any professional services provided by a physician to a patient, including records of the identity, diagnosis, evaluation, or treatment of a patient by a physician that is created or maintained by a physician (*i.e.*, PHI), are confidential and privileged.

69. Under TEX. OCC. CODE § 159.002(c), a person, including a hospital, that receives information from a confidential communication or record as described above, and acts on the patient's behalf, may not disclose such information except to the extent disclosure is consistent with the authorized purposes for which the information was first obtained.

70. St. Joseph's above-described wrongful actions, inaction and/or omissions—to wit, St. Joseph's failure to identify, implement, maintain and monitor the proper data security measures, policies, procedures, controls, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class Members' PII/PHI—directly and/or proximately caused the Data Breach, caused the unauthorized release and disclosure of Plaintiff's and Class Members' PII/PHI, caused Plaintiff and Class Members to suffer economic damages and other actual harm, and collectively constitute the unauthorized release and disclosure of confidential and privileged communications in violation of the Texas Medical Practice Act.

71. Had St. Joseph not engaged in such wrongful actions, inaction and/or omissions, the Data Breach never would have occurred and Plaintiff's and Class Members' PII/PHI would

not have been wrongfully released, disclosed, transferred, sold, opened, read, mined, compromised and otherwise used without their authorization. Plaintiff and Class Members, therefore, request the Court to award them compensation for their economic damages and other actual injury and harm, under TEX. OCC. CODE § 159.009, including, *inter alia*, their (i) actual identity theft, identity fraud and/or medical fraud, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI, (iv) lost benefit of their bargains, (v) deprivation of the full value of their PII/PHI, for which there are well-established national and international markets, (vi) diminished value of the medical services they purchased from St. Joseph, and (vii) the certainly impending and/or increased substantial risk of future economic damages and other actual injury and harm.

72. Plaintiff and Class Members also are entitled to injunctive relief, and further request the Court to order St. Joseph to implement and maintain data security measures, policies, procedures, controls, protocols, and software and hardware systems, including, *inter alia*, (i) strong industry standard encryption algorithms for encryption keys providing access to stored PII/PHI, (ii) using its encryption keys in accordance with industry standards, (iii) immediately encrypting the PII/PHI of its past, present, and future patients and employees within its possession, custody and control, (iv) engaging third-party security auditors/penetration testers and internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on St. Joseph's computer systems on a periodic basis, (v) engaging third-party security auditors and internal personnel to run automated security monitoring, (vi) auditing, testing, and training its security personnel regarding any new or modified procedures, (vii) segmenting consumer data by, among other things, creating firewalls and access controls so that if one area of St. Joseph is compromised, fraudsters cannot gain access to other portions of St.

Joseph's computer systems, (viii) purging, deleting, and destroying in a reasonably secure manner all PII/PHI not necessary for the provision of medical services, (ix) conducting regular database scanning and security checks, (x) regularly evaluating web applications for vulnerabilities to prevent web application threats to St. Joseph's patients and employees, (xi) periodically conducting internal training and education to inform internal data security personnel how to identify and contain a data breach, and the proper data breach response, and (xii) meaningfully educating and protecting its current and former patients and employees about the threats they face as a result of the release and disclosure of their PII/PHI to third parties.

73. Plaintiff and Class Members further request the Court to order St. Joseph to identify and notify all affected Class Members who have not yet been informed of the Data Breach, and notify all affected current or former patients and employees of any future data breaches by email within 24 hours of the discovery of such a breach (or possible breach), and by regular mail within 72 hours.

COUNT II

VIOLATION OF THE TEXAS HOSPITAL LICENSING LAW (TEX. HEALTH & SAFETY CODE § 241.001, et seq.)

74. The previous factual statements and allegations are incorporated by reference.

75. Under TEX. HEALTH & SAFETY CODE § 241.151(2), "health care information" is any information, including payment information, recorded in any form or medium that identifies a patient and relates to the history, diagnosis, treatment, or prognosis of a patient.

76. Under TEX. HEALTH & SAFETY CODE § 241.152(a), except as authorized by TEX. HEALTH & SAFETY CODE § 241.153 (which does not apply here), a hospital or an agent or employee of a hospital may not disclose "health care information" about a patient to any person

other than the patient or the patient's legally authorized representative without the written authorization of the patient or the patient's legally authorized representative.

77. Under TEX. HEALTH & SAFETY CODE § 241.155, a hospital shall adopt and implement reasonable safeguards for the security of all “health care information” it maintains.

78. St. Joseph’s above-described wrongful actions, inaction and/or omissions—to wit, its failure to identify, implement, maintain and monitor the proper data security measures, policies, procedures, controls, protocols, and software and hardware systems to safeguard and protect Plaintiff’s and Class Members’ “health care information” (*i.e.*, their PII/PHI)—directly and/or proximately caused the Data Breach, caused the unauthorized release and disclosure of their PII/PHI, caused them to suffer economic damages and other actual injury and harm, and collectively constitute, *inter alia*, (i) the unauthorized release and disclosure of Plaintiff’s and Class Members’ “health care information” (*i.e.*, their PII/PHI) to unauthorized parties, and (ii) St. Joseph’s failure to adopt and implement reasonable safeguards for the security of their PII/PHI entrusted to it—both of which are violations of the Texas Hospital Licensing Law.

79. Had St. Joseph not engaged in such wrongful actions, inaction and/or omissions, the Data Breach never would have occurred and Plaintiff’s and Class Members’ PII/PHI would not have been wrongfully released, disclosed, transferred, sold, opened, read, mined, compromised and otherwise used without their authorization. Plaintiff and Class Members, therefore, request the Court to award them compensation for their economic damages and other actual injury and harm, under TEX. HEALTH & SAFETY CODE § 241.156, including, *inter alia*, their (i) actual identity theft, identity fraud and/or medical fraud, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI, (iv) lost benefit of their bargains, (v) deprivation of the full value of their PII/PHI, for which there are well-established national and international

markets, (vi) diminished value of the medical services they purchased from St. Joseph, and (vii) the certainly impending and/or increased substantial risk of future economic damages and other actual injury and harm.

80. Plaintiff and Class Members also are entitled to injunctive relief, and further request the Court to order St. Joseph to implement and maintain data security measures, policies, procedures, controls, protocols, and software and hardware systems, including, *inter alia*, (i) strong industry standard encryption algorithms for encryption keys providing access to stored PII/PHI, (ii) using its encryption keys in accordance with industry standards, (iii) immediately encrypting the PII/PHI of its past, present, and future patients and employees within its possession, custody and control, (iv) engaging third-party security auditors/penetration testers and internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on St. Joseph's computer systems on a periodic basis, (v) engaging third-party security auditors and internal personnel to run automated security monitoring, (vi) auditing, testing, and training its security personnel regarding any new or modified procedures, (vii) segmenting consumer data by, among other things, creating firewalls and access controls so that if one area of St. Joseph is compromised, fraudsters cannot gain access to other portions of St. Joseph's computer systems, (viii) purging, deleting, and destroying in a reasonably secure manner all PII/PHI not necessary for the provision of medical services, (ix) conducting regular database scanning and security checks, (x) regularly evaluating web applications for vulnerabilities to prevent web application threats to St. Joseph's patients and employees, (xi) periodically conducting internal training and education to inform internal data security personnel how to identify and contain a data breach, and the proper data breach response, and (xii)

meaningfully educating and protecting its current and former patients and employees about the threats they face as a result of the release and disclosure of their PII/PHI to third parties.

81. Plaintiff and Class Members further request the Court to order St. Joseph to identify and notify all affected Class Members who have not yet been informed of the Data Breach, and notify all affected current or former patients and employees of any future data breaches by email within 24 hours of the discovery of such a breach (or possible breach), and by regular mail within 72 hours.

COUNT III

NEGLIGENCE/GROSS NEGLIGENCE

82. The previous factual statements and allegations are incorporated by reference.

83. Upon St. Joseph coming into possession of Plaintiff's and Class Members' private, confidential, non-public, and sensitive PII/PHI, the Parties entered into a special relationship by which St. Joseph had (and continues to have) a duty to exercise reasonable care in safeguarding and protecting the PII/PHI, and not releasing and disclosing it without authorization. St. Joseph's duty arises from Texas common law, in part, because it was reasonably foreseeable to St. Joseph that because it failed to properly protect the breached server and the PII/PHI contained on the server, a data breach was likely to occur that would release and disclose Plaintiff's and Class Members' PII/PHI without authorization, and cause them to suffer the above-described economic damages and other actual injury and harm. St. Joseph's duty also arises from the PII/PHI data security obligations expressly imposed upon it by, *inter alia*, the Texas Medical Records Privacy Act, the Texas Medical Practice Act, the Texas Hospital Licensing Law, Sections 521.052 and 521.053 of the Texas Business and Commerce Code, and/or the industry standards referenced in its Privacy Notice that St. Joseph claims to "meet or

exceed.” *See* Exhibit B at 3.

84. St. Joseph also had a duty to timely disclose the Data Breach to Plaintiff and Class Members so they could take the appropriate defensive steps necessary to minimize their economic damages and other actual injury and harm. Instead, by its above-described wrongful actions, inaction and/or omissions, and delayed disclosure of the Data Breach, St. Joseph shifted its notification obligation and expenses to Plaintiff and Class Members. St. Joseph also (i) directly and/or proximately caused Plaintiff and Class Members to suffer the above-described economic damages and other actual injury and harm, (ii) saved the cost of implementing the proper patient and employee PII/PHI data security measures, policies, procedures, controls, protocols, and software and hardware systems, and (iii) wrongfully shifted the risk and expense of the Data Breach to Plaintiff and Class Members. St. Joseph’s duty to properly and timely disclose the Data Breach to Plaintiff and Class Members also arises from the same above-described sources.

85. St. Joseph also had a duty to identify, implement, maintain and monitor the appropriate customer data security measures, policies, procedures, controls, protocols, and software and hardware systems within its computer system and servers to prevent and detect data breaches, and the unauthorized release and disclosure of Plaintiff’s and Class Members’ PII/PHI—including their PII/PHI wrongfully released and disclosed in the Data Breach. Such duty also arises from the same above-described sources.

86. St. Joseph, by and through its above-described negligent and/or grossly negligent actions, inaction, and/or omissions, breached its duties to Plaintiff and Class Members by, *inter alia*, failing to identify, implement, maintain and monitor the appropriate data security measures, policies, procedures, controls, protocols, and software and hardware systems within its computer

system and servers, and failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' private, non-public, sensitive PII/PHI within St. Joseph's possession, custody and control, and wrongfully releasing and disclosing their PII/PHI.

87. St. Joseph, by and through its above-described negligent and/or grossly negligent actions, inaction, omissions and/or silence when it had a duty to speak, also breached its duties to Plaintiff and Class Members by failing to (i) advise Plaintiff and Class Members that the appropriate data security measures, policies, procedures, controls, protocols, and software and hardware systems within its computer system and servers, in fact, were not in place, properly functioning and/or monitored, and (ii) timely notify them of the Data Breach so they could take the necessary defensive steps to minimize their economic damages and other actual injury and harm. But for St. Joseph's grossly negligent, negligent and/or wrongful breach of the duties it owed (and continues to owe) Plaintiff and Class Members, their private, confidential, non-public, sensitive PII/PHI would never have been wrongfully released and disclosed without their authorization, compromised, and wrongfully used, the Data Breach would not have occurred, and Plaintiff and Class Members would not have suffered the economic damages and other actual injury and harm they have suffered (and will continue to suffer).

88. The Data Breach and the resulting economic damages and other actual injury and harm suffered by Plaintiff and Class Members were reasonably foreseeable consequences of St. Joseph's negligence and/or gross negligence.

89. The economic loss doctrine does not apply to bar Plaintiff's and Class Members' negligence and/or gross negligence claims because, *inter alia*, (i) St. Joseph is in the business of supplying information for the guidance of Plaintiff and Class Members regarding their health care and/or securing payment from Plaintiff and Class Members for the provision of health care

services, and (ii) St. Joseph made the above-described negligent and/or grossly negligent misrepresentations regarding the data security “tools” it had in place and/or engaged in the above-described negligent and/or grossly negligent conduct.

90. Adding to St. Joseph’s negligence, gross negligence, and violations of the Texas Medical Records Privacy Act, the Texas Medical Practice Act, the Texas Hospital Licensing Law, Sections 521.052 and 521.053 of the Texas Business and Commerce Code, and/or the industry standards referenced in its Privacy Notice that it claims to “meet or exceed” (*see* Privacy Notice (Exhibit B) at 3) is the fact that St. Joseph was on notice that approximately 94% of all healthcare organizations in the United States have recently suffered data breaches.¹¹ This is publicly available information St. Joseph knew, or should have known, that should have prompted St. Joseph to institute the appropriate data security measures, policies, procedures, protocols, and software and hardware systems within its computer system and servers to properly safeguard and protect Plaintiff’s and Class Members’ PII/PHI.

91. St. Joseph’s above-described wrongful actions, inaction and/or omissions—to wit, St. Joseph’s failure to identify, implement, maintain and monitor the proper data security measures, policies, procedures, controls, protocols, and software and hardware systems to safeguard and protect Plaintiff’s and Class Members’ PII/PHI—directly and/or proximately caused the Data Breach, caused the unauthorized release and disclosure of Plaintiff’s and Class Members’ PII/PHI, caused Plaintiff and Class Members to suffer economic damages and other actual injury and harm, and collectively constitute negligence and/or gross negligence at Texas common law. Had St. Joseph not engaged in such wrongful actions, inaction and/or omissions,

¹¹ *Ponemon Study Reveals Ninety-Four Percent of Hospitals Surveyed Suffered Data Breaches* (Dec. 6, 2012), <http://www2.idexpertscorp.com/press/ninety-four-percent-of-hospitals-surveyed-suffered-data-breaches/> (last visited March 7, 2015).

the Data Breach never would have occurred, and Plaintiff's and Class Members' PII/PHI would not have been wrongfully released, disclosed, transferred, sold, opened, read, mined, compromised and otherwise used without their authorization. Plaintiff and Class Members, therefore, request the Court to award them compensation for their economic damages and other actual injury and harm, including, *inter alia*, their (i) actual identity theft, identity fraud and/or medical fraud, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI, (iv) lost benefit of their bargains, (v) deprivation of the full value of their PII/PHI, for which there are well-established national and international markets, (vi) diminished value of the medical services they purchased from St. Joseph, and (vii) the certainly impending and/or increased substantial risk of future economic damages and other actual injury and harm.

92. Plaintiff and Class Members also are entitled to injunctive relief, and further request the Court to order St. Joseph to implement and maintain data security measures, policies, procedures, controls, protocols, and software and hardware systems, including, *inter alia*, (i) strong industry standard encryption algorithms for encryption keys providing access to stored PII/PHI, (ii) using its encryption keys in accordance with industry standards, (iii) immediately encrypting the PII/PHI of its past, present, and future patients and employees within its possession, custody and control, (iv) engaging third-party security auditors/penetration testers and internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on St. Joseph's computer systems on a periodic basis, (v) engaging third-party security auditors and internal personnel to run automated security monitoring, (vi) auditing, testing, and training its security personnel regarding any new or modified procedures, (vii) segmenting consumer data by, among other things, creating firewalls and access controls so that if one area of St. Joseph is compromised, fraudsters cannot gain access to other portions of St.

Joseph's computer systems, (viii) purging, deleting, and destroying in a reasonably secure manner all PII/PHI not necessary for the provision of medical services, (ix) conducting regular database scanning and security checks, (x) regularly evaluating web applications for vulnerabilities to prevent web application threats to St. Joseph's patients and employees, (xi) periodically conducting internal training and education to inform internal data security personnel how to identify and contain a data breach, and the proper data breach response, and (xii) meaningfully educating and protecting its current and former patients and employees about the threats they face as a result of the release and disclosure of their PII/PHI to third parties.

93. Plaintiff and Class Members further request the Court to order St. Joseph to identify and notify all affected Class Members who have not yet been informed of the Data Breach, and notify all affected current or former patients and employees of any future data breaches by email within 24 hours of the discovery of such a breach (or possible breach), and by regular mail within 72 hours.

COUNT IV

NEGLIGENCE *PER SE*

94. The preceding statements and allegations are incorporated by reference.

95. At all relevant times, St. Joseph was required (and continues to be required) to comply with, *inter alia*, the Texas Medical Records Privacy Act, the Texas Medical Practice Act, the Texas Hospital Licensing Law, Sections 521.052 and 521.053 of the Texas Business and Commerce Code, and/or the industry standards referenced in its Privacy Notice that it claims to "meet or exceed" (*see* Privacy Notice (Exhibit B) at 3) requiring it to, *inter alia*, (i) identify, implement, maintain and monitor the appropriate data security measures, policies, procedures, controls, protocols, and software and hardware systems in its computer system and servers, (ii)

safeguard, protect, and not disclose Plaintiff's and Class Members' PII/PHI within its possession, custody and control to unauthorized parties, and (iii) notify Plaintiff and Class Members about the Data Breach as quickly as possible. These statutes and standards establish the duty of care owed by St. Joseph to Plaintiff and Class Members.

96. By its above-described wrongful actions, inaction, omissions—to wit, St. Joseph's failure to identify, implement, maintain and monitor the proper data security measures, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class Members' PII/PHI—the resulting Data Breach, the unauthorized release and disclosure of Plaintiff's and Class Members' PII/PHI, its failure to notify Plaintiff and Class Members that such data security measures, policies, procedures, controls, protocols, and software and hardware systems, in fact, were not in place, operational, and/or monitored, and its failure to timely notify Plaintiff and Class Members about the Data Breach, St. Joseph knowingly, and without excuse, violated the Texas Medical Records Privacy Act, the Texas Medical Practice Act, the Texas Hospital Licensing Law, Sections 521.052 and 521.053 of the Texas Business and Commerce Code, and/or the industry standards referenced in its Privacy Notice that it claims to “meet or exceed” (*see* Privacy Notice (Exhibit B) at 3). Had St. Joseph complied with such laws and standards during the relevant time period, the Data Breach would not have occurred, Plaintiff's and Class Members' PII/PHI would not have been released and disclosed without authorization, they would not have suffered the resulting economic damages and other actual injury and harm, and the Data Breach would have been disclosed to Plaintiff and Class Members at an earlier date.

97. Plaintiff and Class Members are members of the class of persons intended to be protected by the Texas Medical Records Privacy Act, the Texas Medical Practice Act, the Texas Hospital Licensing Law, Sections 521.052 and 521.053 of the Texas Business and Commerce

Code, and/or the industry standards referenced in its Privacy Notice that St. Joseph claims to “meet or exceed.” *See* Privacy Notice (Exhibit B) at 3. The above-described economic damages and other actual injury and harm suffered by Plaintiff and Class Members as a direct and/or proximate result of the Data Breach—for which they are entitled to compensation—are the types of injuries and harm intended to be prevented by these laws and standards.

98. St. Joseph’s above-described wrongful actions, inaction and/or omissions—to wit, its failure to identify, implement, maintain and monitor the proper data security measures, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff’s and Class Members’ PII/PHI—directly and/or proximately caused the Data Breach, caused the unauthorized release and disclosure of their PII/PHI, caused Plaintiff and Class Members to suffer economic damages and other actual injury and harm, and collectively constitute negligence *per se* at Texas common law. Had St. Joseph not engaged in such wrongful actions, inaction and/or omissions, the Data Breach never would have occurred and Plaintiff’s and Class Members’ PII/PHI would not have been wrongfully released, disclosed, transferred, sold, opened, read, mined, compromised and otherwise used without their authorization. Plaintiff and Class Members, therefore, request the Court to award them compensation for their economic damages and other actual injury and harm, including, *inter alia*, their (i) actual identity theft, identity fraud and/or medical fraud, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI, (iv) lost benefit of their bargains, (v) deprivation of the full value of their PII/PHI, for which there are well-established national and international markets, (vi) diminished value of the medical services they purchased from St. Joseph, and (vii) the certainly impending and/or increased substantial risk of future economic damages and other actual injury and harm.

99. Plaintiff and Class Members also are entitled to injunctive relief, and further request the Court to order St. Joseph to implement and maintain data security measures, policies, procedures, controls, protocols, and software and hardware systems, including, *inter alia*, (i) strong industry standard encryption algorithms for encryption keys providing access to stored PII/PHI, (ii) using its encryption keys in accordance with industry standards, (iii) immediately encrypting the PII/PHI of its past, present, and future patients and employees within its possession, custody and control, (iv) engaging third-party security auditors/penetration testers and internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on St. Joseph's computer systems on a periodic basis, (v) engaging third-party security auditors and internal personnel to run automated security monitoring, (vi) auditing, testing, and training its security personnel regarding any new or modified procedures, (vii) segmenting consumer data by, among other things, creating firewalls and access controls so that if one area of St. Joseph is compromised, fraudsters cannot gain access to other portions of St. Joseph's computer systems, (viii) purging, deleting, and destroying in a reasonably secure manner all PII/PHI not necessary for the provision of medical services, (ix) conducting regular database scanning and security checks, (x) regularly evaluating web applications for vulnerabilities to prevent web application threats to St. Joseph's patients and employees, (xi) periodically conducting internal training and education to inform internal data security personnel how to identify and contain a data breach, and the proper data breach response, and (xii) meaningfully educating and protecting its current and former patients and employees about the threats they face as a result of the release and disclosure of their PII/PHI to third parties.

100. Plaintiff and Class Members further request the Court to order St. Joseph to identify and notify all affected Class Members who have not yet been informed of the Data

Breach, and notify all affected current or former patients and employees of any future data breaches by email within 24 hours of the discovery of such a breach (or possible breach), and by regular mail within 72 hours.

COUNT V

BREACH OF CONTRACT

101. The preceding factual statements and allegations are incorporated by reference.

102. Plaintiff and Class Members, on the one hand, and St. Joseph, on the other hand, mutually intended to form and, in fact, formed and entered into valid and enforceable contracts arising from, and evidenced by, the Privacy Notice (Exhibit B). Such contracts govern the Parties' business relationships.

103. Under the terms of such contracts, Plaintiff and Class Members promised to pay (and paid) money to St. Joseph in exchange for health care services, including St. Joseph's protection of their PII/PHI. St. Joseph's contractual obligation to safeguard and protect Plaintiff's and Class Members' PII/PHI, and not release and disclose it without authorization, is a material term of such contracts and continues in full force and effect.

104. All conditions precedent to St. Joseph's liability under these contracts have been performed by Plaintiff and Class Members. Plaintiff and Class Members performed all of their obligations under the contracts by paying St. Joseph for health care services and the protection of their PII/PHI. St. Joseph, however, breached its contracts with Plaintiff and Class Members by knowingly, maliciously, fraudulently, willfully, wantonly, negligently and wrongfully failing to safeguard and protect their PII/PHI, and releasing and disclosing their PII/PHI without authorization, as described above.

105. St. Joseph's above-described wrongful actions, inaction and/or omissions—to wit, St. Joseph's failure to identify, implement, maintain and monitor the proper data security measures, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class Members' PII/PHI—breached its contracts with Plaintiff and Class Members and directly and/or proximately caused them to suffer economic damages and other actual injury and harm in the form of, *inter alia*, the lost benefit of their bargains; to wit, Plaintiff and Class Members understood, agreed, and expected that a portion of the price they paid to St. Joseph for health care services would be spent by St. Joseph to safeguard and protect their PII/PHI—especially in light of St. Joseph's representations and agreements in its Privacy Notice. Although Plaintiff and Class Members paid for the protection of their PII/PHI, St. Joseph failed to do so, thereby resulting in its wrongful release and disclosure to the world without authorization, and Plaintiff's and Class Members' lost benefit of their bargains.

106. St. Joseph's above-described wrongful actions, inaction and/or omissions and the resulting Data breach constitute breach of contract at Texas common law—for which Plaintiff and Class Members are entitled to recover the lost benefit of their bargains.

COUNT VI

BREACH OF IMPLIED CONTRACT

107. The preceding factual statements and allegations are incorporated by reference.

108. In the alternative, Plaintiff and Class Members, on the one hand, and St. Joseph, on the other hand, mutually intended to form and, in fact, formed and entered into valid and enforceable implied contracts arising from, and evidenced by, the Parties' acts and conduct and the Privacy Notice (Exhibit B). Such implied contracts govern the Parties' business relationships, and consist of obligations arising from their mutual agreement and intent to

promise where such agreements and promises are not specifically expressed in words in other agreements, if any.

109. Under the terms of such implied contracts, Plaintiff and Class Members promised to pay (and paid) money to St. Joseph in exchange for health care services, including the protection of their PII/PHI. St. Joseph's contractual obligation to safeguard and protect Plaintiff's and Class Members' PII/PHI is a material term of such implied contracts and continues in full force and effect.

110. All conditions precedent to St. Joseph's liability under these implied contracts have been performed by Plaintiff and Class Members. Plaintiff and Class Members performed all of their obligations under the implied contracts by paying St. Joseph for health care services and the protection of their PII/PHI. St. Joseph, however, breached its implied contracts with Plaintiff and Class Members by knowingly, maliciously, fraudulently, willfully, wantonly, negligently and wrongfully failing to safeguard and protect their PII/PHI, and releasing and disclosing their PII/PHI without authorization, as described above.

111. St. Joseph's above-described wrongful actions, inaction and/or omissions—to wit, St. Joseph's failure to identify, implement, maintain and monitor the proper data security measures, policies, procedures, controls, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class Members' PII/PHI—breached its implied contracts with Plaintiff and Class Members and directly and/or proximately caused them to suffer economic damages and other actual injury and harm in the form of, *inter alia*, the lost benefit of their bargains; to wit, they understood, agreed and expected that a portion of the price they paid to St. Joseph for health care services would be spent by St. Joseph to safeguard and protect their PII/PHI—especially in light of St. Joseph's representations and agreements in its Privacy Notice.

Although Plaintiff and Class Members paid for protection of their PII/PHI, St. Joseph failed to do so, thereby resulting in its wrongful release and disclosure to the world without authorization, and Plaintiff's and Class Members' lost benefit of their bargains. St. Joseph's above-described wrongful actions, inaction and/or omissions constitute breach of implied contract at Texas common law—for which Plaintiff and Class Members are entitled to recover the lost benefit of their bargains.

COUNT VII
VIOLATION OF THE TEXAS DECEPTIVE
TRADE PRACTICES-CONSUMER PROTECTION ACT

112. The preceding factual statements and allegations are incorporated by reference.

113. Plaintiff and Class Members are “consumers” under the Texas Deceptive Trade Practices-Consumer Protection Act (“DTPA”), TEX. BUS. & COM. CODE §17.45(4), by purchasing health care services and PII/PHI protection services from St. Joseph. St. Joseph is a “person” that may be sued under the DTPA, under TEX. BUS. & COM. CODE §17.45(3), for providing such services.

114. By its above-described unconscionable actions and/or unconscionable course of action, inaction and/or omissions, the resulting Data Breach, and the wrongful and unauthorized disclosure of Plaintiff's and Class Members' PII/PHI, St. Joseph knowingly and intentionally engaged in an unconscionable course of action, in violation of TEX. BUS. & COM. CODE §17.50(a)(3), by failing to identify, implement, maintain and monitor the proper data security measures, policies, procedures, controls, protocols, and software and hardware systems to safeguard and protect their PII/PHI—while, at the same time, knowingly, intentionally, and falsely representing in its Privacy Notice that such data security measures, policies, procedures, controls, protocols, and software and hardware systems were in place, operational and/or

monitored (which they were not) (in violation of TEX. BUS. & COM. CODE §17.46(b)(5); (b)(7)—which, as a direct and/or proximate result, was wrongfully released, disclosed, compromised, transferred, sold, opened, read, mined and otherwise used without authorization.

115. St. Joseph's above-described knowing and intentional wrongful actions, inaction and/or omissions and the resulting Data Breach unfairly took advantage of the lack of knowledge, ability, and experience of Plaintiff and Class Members to a grossly unfair degree regarding its computer systems and servers and St. Joseph's inability to safeguard and protect their PII/PHI; to wit, at the time Plaintiff and Class Members gave St. Joseph their PII/PHI in connection with purchasing health care services, they did not know, and had no way of knowing, nor did St. Joseph disclose, that it was incapable of safeguarding and protecting their PII/PHI. In fact, the opposite occurred; St. Joseph falsely represented in its Privacy Notice (Exhibit B) (in violation of TEX. BUS. & COM. CODE §17.46(b)(5);(b)(7)) that it had data security measures, policies, procedures, controls, protocols, and software and hardware systems in place to safeguard and protect Plaintiff's and Class Members' PII/PHI—which admittedly turned out not to be the case. *See* Exhibit A.

116. St. Joseph's above-described knowing and intentional wrongful actions, inaction and/or omissions—to wit, St. Joseph's failure to identify, implement, maintain and monitor the proper data security measures, policies, procedures, controls, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class Members' PII/PHI—directly and/or proximately caused the Data Breach, caused the unauthorized release and disclosure of Plaintiff's and Class Members' PII/PHI, caused them to suffer economic damages and other actual injury and harm, and collectively constitute violations of TEX. BUS. & COM. CODE §17.50(a)(3) and TEX. BUS. & COM. CODE §17.46(b)(5); (b)(7). Had St. Joseph not engaged in

such knowing and intentional wrongful actions, inaction and/or omissions, the Data Breach never would have occurred, and Plaintiff's and Class Members' PII/PHI would not have been wrongfully released, disclosed, compromised, transferred, sold, opened, read, mined and otherwise used without authorization.

117. Plaintiff and Class Members, therefore, request the Court to award them compensation for their economic damages and other actual injury and harm, under Section 17.50 of the Texas Business and Commerce Code, including, *inter alia*, their (i) actual identity theft, identity fraud and/or medical fraud, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI, (iv) lost benefit of their bargains, (v) deprivation of the full value of their PII/PHI, for which there are well-established national and international markets, (vi) diminished value of the medical services they purchased from St. Joseph, and (vii) the certainly impending and/or increased substantial risk of future economic damages and other actual injury and harm.

118. Plaintiff and Class Members also are entitled to injunctive relief, and further request the Court to order St. Joseph to implement and maintain data security measures, policies, procedures, controls, protocols, and software and hardware systems, including, *inter alia*, (i) strong industry standard encryption algorithms for encryption keys providing access to stored PII/PHI, (ii) using its encryption keys in accordance with industry standards, (iii) immediately encrypting the PII/PHI of its past, present, and future patients and employees within its possession, custody and control, (iv) engaging third-party security auditors/penetration testers and internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on St. Joseph's computer systems on a periodic basis, (v) engaging third-party security auditors and internal personnel to run automated security monitoring, (vi) auditing, testing, and training its security personnel regarding any new or modified procedures, (vii)

segmenting consumer data by, among other things, creating firewalls and access controls so that if one area of St. Joseph is compromised, fraudsters cannot gain access to other portions of St. Joseph's computer systems, (viii) purging, deleting, and destroying in a reasonably secure manner all PII/PHI not necessary for the provision of medical services, (ix) conducting regular database scanning and security checks, (x) regularly evaluating web applications for vulnerabilities to prevent web application threats to St. Joseph's patients and employees, (xi) periodically conducting internal training and education to inform internal data security personnel how to identify and contain a data breach, and the proper data breach response, and (xii) meaningfully educating and protecting its current and former patients and employees about the threats they face as a result of the release and disclosure of their PII/PHI to third parties.

119. Plaintiff and Class Members further request the Court to order St. Joseph to identify and notify all affected Class Members who have not yet been informed of the Data Breach, and notify all affected current or former patients and employees of any future data breaches by email within 24 hours of the discovery of such a breach (or possible breach), and by regular mail within 72 hours.

COUNT VIII

INVASION OF PRIVACY

120. The preceding factual statements and allegations are incorporated by reference.

121. St. Joseph's intentional failure to safeguard and protect Plaintiff's and Class Members' PII/PHI, the resulting Data Breach, and unauthorized release and disclosure of their PII/PHI directly and/or proximately resulted in an invasion of their privacy by the public disclosure of such highly confidential and private information without their authorization.

122. Access to Plaintiff's and Class Members' PII/PHI, and the wrongful dissemination of such information into the public domain, was easily achieved because their

PII/PHI (i) was not properly safeguarded and protected within St. Joseph's computer systems, (ii) easily targeted and accessed by fraudsters via the Internet, and, (iii) on information and belief, easily accessed, compromised, bought, sold, disseminated, opened, read, mined and otherwise used without their authorization because the PII/PHI was either improperly encrypted or not encrypted at all.

123. St. Joseph's wrongful release and disclosure of Plaintiff's and Class Members' highly confidential and private PII/PHI to a large group fraudsters and the public at large via the Internet black market, without authorization via the Data Breach, is certain to become (and has become) one of public knowledge, and is not of a legitimate public concern. For the reasons set forth above, St. Joseph's unauthorized release and disclosure of her PII/PHI is, and will continue to be, highly offensive to Plaintiff. Plaintiff further alleges the unauthorized release and disclosure of the above-described highly confidential, privileged, and private PII/PHI also is, and will continue to be, highly offensive to Class Members and other reasonable people.

124. St. Joseph intentionally invaded Plaintiff's and Class Members' privacy by wrongfully releasing and disclosing their PII/PHI to the world without authorization by repeatedly failing and refusing to identify, implement, maintain and/or monitor appropriate data security measures, policies, procedures, controls, protocols, and software and hardware systems to ensure the security and confidentiality of their PII/PHI.

125. St. Joseph's above-described wrongful actions, inaction and/or omissions—to wit, St. Joseph's failure to identify, implement, maintain and monitor the proper data security measures, policies, procedures, controls, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class Members' PII/PHI—directly and/or proximately caused the Data Breach, caused the unauthorized release, disclosure and dissemination to the

world of their PII/PHI, caused Plaintiff and Class Members to suffer economic damages and other actual injury and harm, and collectively constitute an invasion of Plaintiff's and Class Members' privacy at Texas common law by publicly disclosing their private PII/PHI.

126. Had St. Joseph not engaged in such wrongful actions, inaction and/or omissions, the Data Breach never would have occurred and Plaintiff's and Class Members' PII/PHI would not have been wrongfully released, disclosed, transferred, sold, opened, read, mined, compromised and otherwise used without their authorization. Plaintiff and Class Members, therefore, request the Court to award them compensation for their economic damages and other actual injury and harm, including, *inter alia*, their (i) actual identity theft, identity fraud and/or medical fraud, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI, (iv) lost benefit of their bargains, (v) deprivation of the full value of their PII/PHI, for which there are well-established national and international markets, (vi) diminished value of the medical services they purchased from St. Joseph, and (vii) the certainly impending and/or increased substantial risk of future economic damages and other actual injury and harm.

127. Plaintiff and Class Members also are entitled to injunctive relief, and further request the Court to order St. Joseph to implement and maintain data security measures, policies, procedures, controls, protocols, and software and hardware systems, including, *inter alia*, (i) strong industry standard encryption algorithms for encryption keys providing access to stored PII/PHI, (ii) using its encryption keys in accordance with industry standards, (iii) immediately encrypting the PII/PHI of its past, present, and future patients and employees within its possession, custody and control, (iv) engaging third-party security auditors/penetration testers and internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on St. Joseph's computer systems on a periodic basis, (v) engaging third-party

security auditors and internal personnel to run automated security monitoring, (vi) auditing, testing, and training its security personnel regarding any new or modified procedures, (vii) segmenting consumer data by, among other things, creating firewalls and access controls so that if one area of St. Joseph is compromised, fraudsters cannot gain access to other portions of St. Joseph's computer systems, (viii) purging, deleting, and destroying in a reasonably secure manner all PII/PHI not necessary for the provision of medical services, (ix) conducting regular database scanning and security checks, (x) regularly evaluating web applications for vulnerabilities to prevent web application threats to St. Joseph's patients and employees, (xi) periodically conducting internal training and education to inform internal data security personnel how to identify and contain a data breach, and the proper data breach response, and (xii) meaningfully educating and protecting its current and former patients and employees about the threats they face as a result of the release and disclosure of their PII/PHI to third parties.

128. Plaintiff and Class Members further request the Court to order St. Joseph to identify and notify all affected Class Members who have not yet been informed of the Data Breach, and notify all affected current or former patients and employees of any future data breaches by email within 24 hours of the discovery of such a breach (or possible breach), and by regular mail within 72 hours.

COUNT IX

BREACH OF FIDUCIARY DUTY

129. The preceding factual statements and allegations are incorporated by reference.

130. Pursuant to TEX. OCC. CODE § 159.002(a);(b), communications between a physician and a patient, relative to or in connection with any professional services provided by a physician to a patient, including records of the identity, diagnosis, evaluation, or treatment of a

patient by a physician created or maintained by a physician—such as Plaintiff’s and Class Members’ PII/PHI—are confidential and privileged.

131. Pursuant to TEX. OCC. CODE § 159.002(c), a person, including a hospital, that receives information from a confidential communication or record as described above, and acts on the patient's behalf, may not release or disclose such information except to the extent the release or disclosure is consistent with the authorized purposes for which the information was first obtained.

132. Pursuant to TEX. HEALTH & SAFETY CODE § 241.151(2), “health care information” is any information, including payment information, recorded in any form or medium, that identifies a patient and relates to the history, diagnosis, treatment, or prognosis of a patient—such as Plaintiff’s and Class Members’ PII/PHI.

133. Pursuant to TEX. HEALTH & SAFETY CODE § 241.152(a), except as authorized by TEX. HEALTH & SAFETY CODE § 241.153 (which does not apply here), a hospital or an agent or employee of a hospital may not release or disclose “health care information” about a patient—such as Plaintiff’s and Class Members’ PII/PHI—to any person other than the patient or the patient's legally authorized representative without the written authorization of the patient or the patient's legally authorized representative.

134. The unique, personal, private, and highly confidential nature of PII/PHI itself, including the PII/PHI entrusted by Plaintiff and Class Members to St. Joseph, and the absolute duty to safeguard and protect PII/PHI imposed on St. Joseph by the above statutes, as well as Sections 521.052 and 521.053 of the Texas Business and Commerce Code, and/or the industry standards referenced in its Privacy Notice that it claims to “meet or exceed” (*see* Exhibit B at 3),

confirm that St. Joseph was (and continues to be) in personal, confidential and fiduciary relationships with Plaintiff and Class Members as a matter of Texas law.

135. As a fiduciary, St. Joseph owed (and continues to owe) Plaintiff and Class Members (i) the commitment to deal fairly and honestly, (ii) the duties of good faith and undivided loyalty, and (iii) integrity of the strictest kind. St. Joseph was (and continues to be) obligated to exercise the highest degree of care in carrying out its obligations to Plaintiff and Class Members under the Parties' confidential, special and fiduciary relationships including, without limitation, safeguarding and protecting Plaintiff's and Class Members' PII/PHI, and not releasing or disclosing the PII/PHI without authorization.

136. St. Joseph breached its fiduciary duties to Plaintiff and Class Members by failing to identify, implement, maintain and/or monitor appropriate data security measures, policies, procedures, controls, protocols, and software and hardware systems to ensure the security and confidentiality of Plaintiff's and Class Members' PII/PHI, and wrongfully releasing and disclosing their PII/PHI without authorization, as described above. St. Joseph also breached its fiduciary duties to Plaintiff and Class Members by failing to failing to (i) advise Plaintiff and Class Members that the appropriate data security measures, policies, procedures, controls, protocols, and software and hardware systems within its computer systems and servers, in fact, were not in place, properly functioning and/or monitored (but misrepresenting the exact opposite in the Privacy Notice), and (ii) timely notify them of the Data Breach so they could take the necessary defensive steps to minimize their economic damages and other actual injury and harm.

137. To the extent either of the Defendants is a fiduciary that did not breach its fiduciary duties to Plaintiff and Class Members, such Defendant is nonetheless liable because it

had knowledge of the breaches of fiduciary duties committed by the other fiduciary, and did not make reasonable efforts to prevent and/or remedy such fiduciary breaches.

138. St. Joseph willfully and wantonly breached its fiduciary duties to Plaintiff and Class Members or, at the very least, committed these breaches with conscious indifference and reckless disregard of their rights and interests.

139. St. Joseph's above-described wrongful actions, inaction and/or omissions directly and/or proximately caused the Data Breach, caused the unauthorized release and disclosure of Plaintiff's and Class Members' PII/PHI, caused Plaintiff and Class Members to suffer economic damages and other actual injury and harm, and collectively constitute breach of fiduciary duty at Texas common law. Had St. Joseph not engaged in such wrongful actions, inaction and/or omissions, the Data Breach never would have occurred and Plaintiff's and Class Members' PII/PHI would not have been wrongfully released, disclosed, transferred, sold, opened, read, mined, compromised and otherwise used without their authorization. Plaintiff and Class Members, therefore, request the Court to award them compensation for their economic damages and other actual injury and harm, including, *inter alia*, their (i) actual identity theft, identity fraud and/or medical fraud, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI, (iv) lost benefit of their bargains, (v) deprivation of the full value of their PII/PHI, for which there are well-established national and international markets, (vi) diminished value of the medical services they purchased from St. Joseph, and (vii) the certainly impending and/or increased substantial risk of future economic damages and other actual injury and harm.

140. Plaintiff and Class Members also are entitled to injunctive relief, and further request the Court to order St. Joseph to implement and maintain data security measures, policies, procedures, controls, protocols, and software and hardware systems, including, *inter alia*, (i)

strong industry standard encryption algorithms for encryption keys providing access to stored PII/PHI, (ii) using its encryption keys in accordance with industry standards, (iii) immediately encrypting the PII/PHI of its past, present, and future patients and employees within its possession, custody and control, (iv) engaging third-party security auditors/penetration testers and internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on St. Joseph's computer systems on a periodic basis, (v) engaging third-party security auditors and internal personnel to run automated security monitoring, (vi) auditing, testing, and training its security personnel regarding any new or modified procedures, (vii) segmenting consumer data by, among other things, creating firewalls and access controls so that if one area of St. Joseph is compromised, fraudsters cannot gain access to other portions of St. Joseph's computer systems, (viii) purging, deleting, and destroying in a reasonably secure manner all PII/PHI not necessary for the provision of medical services, (ix) conducting regular database scanning and security checks, (x) regularly evaluating web applications for vulnerabilities to prevent web application threats to St. Joseph's patients and employees, (xi) periodically conducting internal training and education to inform internal data security personnel how to identify and contain a data breach, and the proper data breach response, and (xii) meaningfully educating and protecting its current and former patients and employees about the threats they face as a result of the release and disclosure of their PII/PHI to third parties.

141. Plaintiff and Class Members further request the Court to order St. Joseph to identify and notify all affected Class Members who have not yet been informed of the Data Breach, and notify all affected current or former patients and employees of any future data breaches by email within 24 hours of the discovery of such a breach (or possible breach), and by regular mail within 72 hours.

COUNT X

BREACH OF CONFIDENTIALITY

142. The preceding factual statements and allegations are incorporated by reference.

143. Plaintiff's and Class Members' unique, personal, and private PII/PHI delivered to St. Joseph for safekeeping (at St. Joseph's request) was (and continues to be) highly confidential.

144. St. Joseph breached the confidentiality of Plaintiff's and Class Members' PII/PHI by failing to identify, implement, maintain and/or monitor appropriate data security measures, policies, procedures, controls, protocols, and software and hardware systems to ensure the security and confidentiality of Plaintiff's and Class Members' PII/PHI, and wrongfully releasing and disclosing their PII/PHI without authorization, as described above.

145. St. Joseph's above-described wrongful actions, inaction and/or omissions—to wit, St. Joseph's failure to identify, implement, maintain and monitor the proper data security measures, policies, procedures, controls, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class Members' PII/PHI—directly and/or proximately caused the Data Breach, caused the unauthorized release and disclosure of Plaintiff's and Class Members' PII/PHI, caused Plaintiff and Class Members to suffer economic damages and other actual injury and harm, and collectively constitute breach of confidentiality at Texas common law.

146. Had St. Joseph not engaged in such wrongful actions, inaction and/or omissions, the Data Breach never would have occurred and Plaintiff's and Class Members' PII/PHI would not have been wrongfully released, disclosed, transferred, sold, opened, read, mined, compromised and otherwise used without their authorization. Plaintiff and Class Members, therefore, request the Court to award them compensation for their economic damages and other actual injury and harm, including, *inter alia*, their (i) actual identity theft, identity fraud and/or medical fraud, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI, (iv) lost

benefit of their bargains, (v) deprivation of the full value of their PII/PHI, for which there are well-established national and international markets, (vi) diminished value of the medical services they purchased from St. Joseph, and (vii) the certainly impending and/or increased substantial risk of future economic damages and other actual injury and harm.

147. Plaintiff and Class Members also are entitled to injunctive relief, and further request the Court to order St. Joseph to implement and maintain data security measures, policies, procedures, controls, protocols, and software and hardware systems, including, *inter alia*, (i) strong industry standard encryption algorithms for encryption keys providing access to stored PII/PHI, (ii) using its encryption keys in accordance with industry standards, (iii) immediately encrypting the PII/PHI of its past, present, and future patients and employees within its possession, custody and control, (iv) engaging third-party security auditors/penetration testers and internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on St. Joseph's computer systems on a periodic basis, (v) engaging third-party security auditors and internal personnel to run automated security monitoring, (vi) auditing, testing, and training its security personnel regarding any new or modified procedures, (vii) segmenting consumer data by, among other things, creating firewalls and access controls so that if one area of St. Joseph is compromised, fraudsters cannot gain access to other portions of St. Joseph's computer systems, (viii) purging, deleting, and destroying in a reasonably secure manner all PII/PHI not necessary for the provision of medical services, (ix) conducting regular database scanning and security checks, (x) regularly evaluating web applications for vulnerabilities to prevent web application threats to St. Joseph's patients and employees, (xi) periodically conducting internal training and education to inform internal data security personnel how to identify and contain a data breach, and the proper data breach response, and (xii)

meaningfully educating and protecting its current and former patients and employees about the threats they face as a result of the release and disclosure of their PII/PHI to third parties.

148. Plaintiff and Class Members further request the Court to order St. Joseph to identify and notify all affected Class Members who have not yet been informed of the Data Breach, and notify all affected current or former patients and employees of any future data breaches by email within 24 hours of the discovery of such a breach (or possible breach), and by regular mail within 72 hours.

COUNT XI

MONEY HAD AND RECEIVED/ASSUMPSIT

149. The preceding factual statements and allegations are incorporated by reference.

150. Plaintiff pleads this Count in the alternative to its breach of contract claims because Plaintiff and Class Members cannot recover under this Count and under their breach of contract counts.

151. By its above-described wrongful actions, inaction and/or omissions—to wit, St. Joseph's failure to identify, implement, maintain and monitor the proper data security measures, policies, procedures, controls, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class Members' PII/PHI, the resulting Data Breach, and the unauthorized release and disclosure of their PII/PHI—St. Joseph holds money conferred on it by Plaintiff and Class Members (*i.e.*, that portion of the health services purchase prices they paid St. Joseph for protecting their PII/PHI, which St. Joseph admittedly failed to do). *See* Exhibit A. St. Joseph has been unjustly enriched by the funds it received from Plaintiff and Class Members that it should have spent to safeguard and protect their PII/PHI which, in equity and good conscience, belongs to them, and should be refunded, because St. Joseph failed to do so.

152. St. Joseph also continues to be unjustly enriched by, *inter alia*, (i) the saved cost of implementing the proper PII/PHI security measures, policies, procedures, controls, protocols, and software and hardware systems in its computer systems and servers, which it did not implement, (ii) the shifted risk and expense of the Data Breach to Plaintiff and Class Members, and (iii) the return on investment on all of the above-described amounts.

153. St. Joseph, therefore, should be compelled to refund (or disgorge) such wrongfully collected, saved back and/or shifted funds and expenses under the common law equitable doctrine of money had and received and/or the duty to make restitution under the common law equitable doctrine of *assumpsit*.

RELIEF REQUESTED

154. The preceding factual statements and allegations are incorporated by reference.

155. **ACTUAL, CONSEQUENTIAL DAMAGES AND/OR NOMINAL DAMAGES.** As a direct and/or proximate result of St. Joseph's wrongful actions and/or inaction, the resulting Data Breach, and St. Joseph's wrongful release and disclosure of their PII/PHI without authorization, Plaintiff and Class Members have suffered (and continue to suffer) economic damages and other actual injury and harm in the form of, *inter alia*, (i) actual identity theft, identity fraud and/or medical fraud, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI, (iv) lost benefit of their bargains, (v) deprivation of the full value of their PII/PHI, for which there are well-established national and international markets, (vi) diminished value of the medical services they purchased from St. Joseph, and (vii) the certainly impending and/or increased substantial risk of future economic damages and other actual injury and harm—for which they are entitled to compensation. Plaintiff's and Class Members' damages were foreseeable by St. Joseph and

exceed the minimum jurisdictional limits of this Court. All conditions precedent to Plaintiff's and Class Members' claims for relief have been performed and/or occurred.

156. **EXEMPLARY DAMAGES.** Plaintiff and Class Members also are entitled to exemplary damages as punishment and to deter such wrongful actions, inaction and/or omissions in the future. All conditions precedent to Plaintiff's and Class Members' claims for relief have been performed and/or occurred.

157. **DTPA TREBLE DAMAGES.** Plaintiff and Class Members also are entitled to treble damages for St. Joseph's knowing, willful, intentional, wrongful and unconscionable conduct, in violation of TEX. BUS. & COM. CODE §17.50(a)(3) and §17.46(b)(5);(b)(7), under TEX. BUS. & COM. CODE §17.50(b)(1). All conditions precedent to Plaintiff's and Class Members' claims for relief have been performed and/or occurred.

158. **INJUNCTIVE RELIEF.** Pursuant to, *inter alia*, the Texas Medical Practice Act, TEX. OCC. CODE §159.009(a), and the Texas Hospital Licensing Law, TEX. HEALTH & SAFETY CODE §241.156(a)(1), Plaintiff and Class Members also are entitled to injunctive relief requiring St. Joseph to immediately disclose to Plaintiff and Class Members the precise nature, breadth, scope and extent of their wrongfully released, disclosed, and compromised PII/PHI, including the specific information comprising the wrongfully released and disclosed "medical information." Plaintiff and Class Members also are entitled to injunctive relief requiring St. Joseph to implement and maintain data security measures, policies, procedures, controls, protocols, and software and hardware systems, including, *inter alia*, (i) strong industry standard encryption algorithms for encryption keys providing access to stored PII/PHI, (ii) using its encryption keys in accordance with industry standards, (iii) immediately encrypting the PII/PHI of its past, present, and future patients and employees within its possession, custody and control, (iv) engaging third-party

security auditors/penetration testers and internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on St. Joseph's computer systems on a periodic basis, (v) engaging third-party security auditors and internal personnel to run automated security monitoring, (vi) auditing, testing, and training its security personnel regarding any new or modified procedures, (vii) segmenting consumer data by, among other things, creating firewalls and access controls so that if one area of St. Joseph is compromised, fraudsters cannot gain access to other portions of St. Joseph's computer systems, (viii) purging, deleting, and destroying in a reasonably secure manner all PII/PHI not necessary for the provision of medical services, (ix) conducting regular database scanning and security checks, (x) regularly evaluating web applications for vulnerabilities to prevent web application threats to St. Joseph's patients and employees, (xi) periodically conducting internal training and education to inform internal data security personnel how to identify and contain a data breach, and the proper data breach response, and (xii) meaningfully educating and protecting its current and former patients and employees about the threats they face as a result of the release and disclosure of their PII/PHI to third parties. Plaintiff and Class Members also are entitled to injunctive relief requiring St. Joseph to identify and notify all affected Class Members who have not yet been informed of the Data Breach, and notify all affected current or former patients and employees of any future data breaches by email within 24 hours of the discovery of such a breach (or possible breach), and by regular mail within 72 hours. All conditions precedent to Plaintiff's and Class Members' claims for relief have been performed and/or occurred. Pursuant to the Texas Medical Practice Act, TEX. OCC. CODE §159.009(a), and the Texas Hospital Licensing Law, TEX. HEALTH & SAFETY CODE §241.156(c), Plaintiff's request for injunctive relief takes precedence over all civil matters on the Court's docket except those matters to which equal precedence is granted by law.

159. **ATTORNEYS' FEES, LITIGATION EXPENSES AND COSTS.** Plaintiff and Class Members also are entitled to recover their attorneys' fees, litigation expenses and court costs in prosecuting this action pursuant to, *inter alia*, (i) TEX. CIV. PRAC. & REM. CODE Chapter 38, and (ii) TEX. BUS. & COM. CODE §17.50(d). All conditions precedent to Plaintiff's and Class Members' claims for relief have been performed and/or occurred.

WHEREFORE, Plaintiff, on behalf of herself and Class Members, respectfully requests that (i) St. Joseph be cited to appear and answer this lawsuit, (ii) this action be certified as a class action, (iii) Plaintiff be designated the Class Representative, and (iv) Plaintiff's counsel be appointed Class Counsel. Plaintiff further requests that upon final trial or hearing, judgment be awarded against St. Joseph, in favor of Plaintiff and Class Members, for:

- (i) actual damages, consequential damages, and/or nominal damages (as described above) in an amount to be determined by the trier of fact;
- (ii) exemplary damages;
- (iii) treble damages as set forth above;
- (iv) injunctive relief as set forth above;
- (v) pre- and post-judgment interest at the highest applicable legal rates;
- (vi) attorneys' fees and litigation expenses incurred through trial and any appeals;
- (vii) costs of suit; and
- (viii) such other and further relief the Court deems just and proper.

JURY DEMAND

Plaintiff, on behalf of herself and all others similarly situated, respectfully demands a trial by jury on all of her claims and causes of action so triable.

Date: March 12, 2015

Respectfully submitted,

/s/ Richard L. Coffman

Richard L. Coffman
Texas Bar No. 04497460
THE COFFMAN LAW FIRM
505 Orleans St., Ste. 505
Beaumont, TX 77701
Telephone: (409) 833-7700
Facsimile: (866) 835-8250
Email: rcoffman@coffmanlawfirm.com

Bruno A. Shimek
Texas Bar No. 18625550
218 North Main Street
Bryan, TX 77803
Telephone: (979) 220-2479
Facsimile: (979) 823-3327
Email: bshimeklaw@gmail.com

Mitchell A. Toups
Texas Bar No. 20151600
WELLER, GREEN, TOUPS & TERRELL, LLP
2615 Calder Ave., Suite 400
Beaumont, TX 77702
Telephone: (409) 838-0101
Facsimile: (409) 838-6780
Email: matoups@wgttlaw.com

Jason Webster
Texas Bar No. 24033318
THE WEBSTER LAW FIRM
6200 Savoy, Suite 515
Houston, TX 77036
Telephone: (713) 581-3900
Facsimile: (713) 409-6464
Email: jwebster@thewebsterlawfirm.com

Conrad Day
Texas Bar No. 05607550
18 West Main
Bellville, TX 77418
Telephone: (979) 865-9103
Facsimile: (979) 865-9104
Email: conrad@conradday.com

EXHIBIT A



Processing Center • P.O. Box 3825 • Suwanee, GA 30024



240 1 69582 *****AUTO**5-DIGIT 77868

Beverly Peters
10925 Tegeler Rd
Brenham, TX 77833-8248

February 4, 2014



Dear Beverly Peters,*

St. Joseph Health System ("SJHS") based in Bryan, Texas, is writing to inform you of an incident that may affect your personal information.

Between Monday, December 16 and Wednesday, December 18, 2013, SJHS experienced a security attack in which hackers gained unauthorized access to one server on its computer system. SJHS acted quickly, shutting down access to the involved computer on December 18, and hiring national security and computer forensics experts to thoroughly investigate this matter. Our investigation, which is ongoing, determined that this security attack may have resulted in unauthorized access to records for some SJHS patients, employees, and some employees' beneficiaries. These records include your name, medical information and possibly your address.

While it is possible that some information was accessed or taken, the forensics investigation has been unable to confirm this, which is why we are providing this notice to you. The computer was shut down when we discovered the security attack on December 18, 2013, so we believe the potential risk to your information ended on that date. SJHS is working with the United States Federal Bureau of Investigation, which is also looking into this incident.

It is important to note that SJHS has received no reports that any of your personal information has been misused. We take this matter, and the security of your personal information, very seriously. As a precaution, SJHS wants to assist you in protecting your identity even though we are not aware of any misuse of your information and we have been unable to determine whether any data was in fact taken. SJHS has also hired AllClear ID to protect your identity for 12 months at no cost to you. These identity protection services start on the date of this notice and can be used any time over the next 12 months.

- AllClear SECURE: The team at AllClear ID is ready and standing by if you would like help protecting your identity. You are automatically eligible to use this service - there is no action required on your part. If a problem arises, simply call (855) 731-6011 and a dedicated investigator will do the work to recover financial losses, restore your credit and make sure your identity is returned to its proper condition. AllClear maintains an A+ rating at the Better Business Bureau.

*Si Usted prefiere hablar con alguien en Español sobre este asunto, por favor comuníquese con el centro confidencial de soporte al cliente, por llamada gratiz, (855) 731-6011.



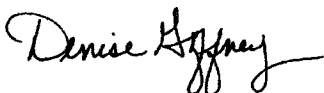
- AllClear PRO: This service offers additional layers of protection including credit monitoring and a \$1 million identity theft insurance policy. To use the PRO service, you will need to sign-up online at enroll.allclearid.com, or by phone by calling (855) 731-6011 using the following redemption code: **1306833540**. To enroll in this free additional service, you will need to provide your personal information to AllClear ID.

To further protect yourself from identity theft or financial loss, we encourage you to remain vigilant, to review your account statements, and to monitor your credit reports and explanation of benefits forms for suspicious activity. You can also check your credit by obtaining a free credit report. Under U.S. law, you are entitled to one free credit report every year from each of the three major credit bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also write, call, or email the three major credit bureaus directly to ask for a free copy of your credit report. Additional information regarding how to contact the credit bureaus and how you may protect your identity is included on the attached document titled "Information About Identity Theft Prevention."

We are sorry for any trouble or concern that this may have caused you. If you have any questions about this incident or this letter, or if you believe you may be a victim of identity theft please contact the call center. The center is confidential, and staffed by professionals trained in identity and credit protection. **You may reach the confidential call center by dialing, toll-free, (855) 731-6011**, Monday through Saturday, 8:00 AM to 8:00 PM U.S. Central Time, excluding major holidays.

Please rest assured that we are taking steps that will prevent this from happening again in the future. We encourage you to take advantage of the free identity and credit protection services described above. SJHS remains committed to the security of your personal information.

Sincerely,



Denise Goffney, Corporate Compliance Officer and Privacy Officer
St. Joseph Health System

Information About Identity Theft Prevention

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax, P.O. Box 740241, Atlanta, Georgia 30374-0241, 1-800-685-1111, www.equifax.com

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

TransUnion, P.O. Box 2000, Chester, PA 19022, 1-800-916-8800, www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

Federal Trade Commission, Consumer Response Center

600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General, Consumer Protection Division

200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

For residents of Massachusetts: You also have the right to obtain a police report.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division

9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

We recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive regular explanation of benefits statements, you may contact your provider and request them to send such statements following the provision of services in your name or number.

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the

appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax: 1-800-525-6285, www.equifax.com

Experian: 1-888-397-3742, www.experian.com

TransUnion: 1-800-680-7289, www.transunion.com

Credit Freezes (for Non-Massachusetts Residents): You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally \$5 to \$20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax, P.O. Box 105788, Atlanta, GA 30348, www.equifax.com

Experian, P.O. Box 9554, Allen, TX 75013, www.experian.com

TransUnion, P.O. Box 2000, Chester, PA 19022, www.transunion.com

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

Credit Freezes (for Massachusetts Residents): Massachusetts law gives you the right to place a security freeze on your consumer reports. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. Using a security freeze, however, may delay your ability to obtain credit. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below:

Equifax, P.O. Box 105788, Atlanta, GA 30348, www.equifax.com

Experian, P.O. Box 9554, Allen, TX 75013, www.experian.com

TransUnion, P.O. Box 2000, Chester, PA 19022, www.transunion.com

Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent). The credit reporting company may charge a reasonable fee of up to \$5 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a valid police report relating to the identity theft to the credit reporting company.

AllClear Secure Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- Automatic 12 months of coverage
- No cost to you – ever. AllClear Secure is paid for by the participating Company.

Services Provided

If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services ("Services") to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Secure is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period

You are automatically protected for 12 months from the date the breach incident occurred, as communicated in the breach notification letter you received from Company (the "Coverage Period"). Fraud Events that occurred prior to your Coverage Period are not covered by AllClear Secure services.

Eligibility Requirements

To be eligible for Services under AllClear Secure coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older, reside in the United States, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim

If you become a victim of fraud covered by the AllClear Secure services, you must:

- Notify AllClear ID by calling 1.855.434.8075 to report the fraud prior to expiration of your Coverage Period.
- Provide proof of eligibility for AllClear Secure by providing the redemption code on the notification letter you received from the sponsor Company.
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require;
- Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft;

Coverage under AllClear Secure Does Not Apply to the Following:

Any expense, damage or loss:

- Due to
 - Any transactions on your financial accounts made by authorized users, even if acting without your knowledge
 - Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your "Misrepresentation")
- Incurred by you from an Event that did not occur during your coverage period;
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Secure coverage period.

Other Exclusions:

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity;
- AllClear ID is not an insurance company, and AllClear Secure is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur; and
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud;
- You are expected to protect your personal information in a reasonable way at all times. Accordingly, you will not recklessly disclose or publish your Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information, such as, by way of example, in response to "phishing" scams, unsolicited emails, or pop-up messages seeking disclosure of personal information.

Opt-out Policy

If for any reason you wish to have your information removed from the eligibility database for AllClear Secure, please contact AllClear ID:

E-mail support@allclearid.com	Mail AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	Phone 1.855.434.8077
---	--	--------------------------------

EXHIBIT B

Notice of Privacy Practices



Applicability of Notice

This Notice describes the privacy practices of St. Joseph Health System and its Affiliated Facilities/Entities which are set forth below. Each of these entities are separate legal entities, but they operate as an organized health care arrangement for HIPAA purposes. For the purpose of this Notice, the terms “St. Joseph,” “we” and “our” refer to St. Joseph Health System and its Affiliated Facilities/Entities only with reference to health information generated or maintained at the locations set forth below and our privacy practices regarding such information. The Effective Date of this Notice is September 1, 2011.

Privacy Obligations

St. Joseph is required by law to maintain the privacy of health information about you that can identify you (“Protected Health Information” or “PHI”), to provide you with this Notice of our legal duties and privacy practices with respect to your PHI, and to abide by the terms of the Notice currently in effect. We reserve the right to change this Notice. We reserve the right to make the revised or changed Notice effective for medical information we already have about you as well as any information we receive in the future. We will post a copy of the current Notice in each of the locations identified below. The Notice will contain the effective date. A copy of the current Notice will be made available to you when you initially register with an Affiliated Entity for treatment or services, upon your request, and on subsequent visits if the Notice has been revised.

Our Pledge

We understand that all information about you and your health is personal. We are committed to protecting this information. When you receive services at a St. Joseph Facility/Entity, a medical record is created. This record describes the services provided to you and is needed to provide you with quality care and to comply with certain legal requirements. This Notice applies to records of your care generated by St. Joseph, whether made by a St. Joseph employee or a physician involved in your care. Physicians may have different policies regarding medical information created in their office. This Notice tells you about the ways in which we may use and disclose your medical information. It also describes your rights and certain obligations we have regarding the use and disclosure of your medical information. If you have any questions you may contact our Chief Compliance and Privacy Officer, 2801 Franciscan Drive, Bryan, Texas, 77802 (979-776-5316).

How We May Use and Disclose Your Health Information

The following information describes how we are permitted, or required by law, to use and disclose your Protected Health Information:

Permissible Uses and Disclosures without Your Written Authorization

In certain situations, which are described below, your written authorization must be obtained in order to use and/or disclose your PHI. However, St. Joseph does not need an authorization from you for the following uses and disclosures:

Uses and Disclosures for Treatment, Payment and Health Care

Operations: Your PHI may be used to treat you, to obtain payment for services provided to you, and to conduct “health care operations” as described below:

Treatment: Your PHI may be used and disclosed to provide treatment and other services to you -- for example to diagnose and treat your injury or illness. In addition, you may be contacted to provide appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest to you. Your PHI may also be disclosed to physicians, organizations or individuals outside of St. Joseph but who are also part of your healthcare team.

Payment: Your PHI may be used and disclosed to your insurance company or other third party to collect payment for services. For example, we may need to give your health plan information about surgery you received while here so that they will pay us or reimburse you. We may also tell your health plan about a treatment you are going to receive to obtain prior approval or to determine whether your plan will cover the treatment.

Health Care Operations: Your PHI may be used and disclosed in connection with our health care operations. For example, your PHI may be 1) used to evaluate the quality and competence of physicians, nurses and other health care workers; or 2) combined with others' information to determine the community need for services or effectiveness of treatment. We may also disclose this information to doctors, nurses, technicians, health care students or management for review and learning purposes and to business associates who perform treatment, payment and health care operations services on behalf of St. Joseph.

Sharing Information with Another Organization: Your PHI may also be shared with another organization if 1) it is involved or may be involved in your care; 2) it is or may be involved in the payment of your care; or 3) such organization already has relations with you and the information shared will help both of our organizations to conduct quality assurance activities, population-based activities, case management, care coordination, training, accreditation, licensing or credentialing, or for health care fraud and abuse detection or compliance. We may, for example 1) share your information with several home health agencies as we attempt to identify the best one for you or; 2) share your information with companies that will assist us in obtaining payment or; 3) share your information with an organization that will assist us in measuring and improving our quality of care.

Use and Disclosure for Directory of Individuals in the Hospital: St. Joseph may include your name, location in the hospital, general health condition (e.g. fair, stable, etc.), and religious affiliation in a patient directory without obtaining your authorization unless you object to inclusion in the directory. This information, except for your religious affiliation, may also be released to people who ask for you by name. Your religious affiliation may be given to a member of the clergy, even if they don't ask for you by name. This is so your family, friends and clergy can visit you in the facility and generally know how you are doing.

Disclosure to Relatives and Close Friends: Your PHI may be disclosed to a family member, friend or other person to the extent necessary to help with your health care or with payment for your health care. We may use or disclose your name, hospital location, and general condition or death to notify, or assist in the notification of (including identifying or locating) a person involved in your care. We may also disclose your medical information to whomever you give us permission. Before we disclose your medical information to a person involved in your health care or payment for your health care, we will provide you with an opportunity to object to such uses or disclosures. If you are not present, or in the event of your incapacity or an emergency, we will disclose your medical information based on our professional judgment of whether the disclosure would be in your best interest. We will also use our professional judgment and our experience with common practice to allow a person to pick up filled prescriptions, medical supplies or other similar forms of medical information.

Disaster Relief: Your PHI may be used or disclosed to a public or private entity authorized by law or by its charter to assist in disaster relief efforts.

Research: Under certain circumstances, we may use and disclose medical information about you for research purposes. For example, a research project may involve comparing the health and recovery of all patients who received one medication to those who received another, for the same condition. All research projects are subject to special approval by the Institutional Review Board. We may disclose medical information about you to people preparing to conduct a research project so long as this information does not leave St. Joseph. For example, a prospective researcher may want to look at patients with specific medical needs. If the research involves anything more than a review of your medical information, we will contact you in order to obtain your authorization or its further use will be subject to your authorization. Some research involves a review of medical care only (record review). In this research, the risk of physical harm or injury to the patient is small and the need for an informed consent from the patient is waived. Research involving a record review must be approved by the Institutional Review Board. If approved, the Ethics Committee will also review the proposed research to ensure the privacy interests of the patients are protected.

Fundraising Activities: St. Joseph may use or disclose health information about you to contact you in an effort to raise money for our organization and its operations. We may disclose this information to the St. Joseph Foundation to assist us in our fundraising activities. Only contact information such as your name, address and telephone number, and the dates you received treatment or services at St. Joseph would be released. You have the right to opt out of fundraising communications at any time and your request must be honored. If you would like to opt-out of receiving fundraising communications, please call 1-877-367-5681 to make your opt-out request.

As Required by Law: We will disclose medical information about you when required to do so by federal, state or local law.

Public Health Activities: Your PHI may be disclosed as authorized by law for public health activities. These activities generally include providing information to/for:

- Disease and vital statistics reporting, child abuse reporting, adult protective services and FDA oversight
- Employers regarding work-related illness or injury
- Cancer, Trauma and Birth Registries
- Health Oversight Agencies (for such things as audits, inspections, and licensure)

- Responding to court and administrative orders and for other lawful processes
- Requests from law enforcement officials pursuant to subpoenas and other lawful processes, concerning crime victims, suspicious deaths, crimes on our premises, reporting crimes in emergencies, and for purposes of identifying or locating a suspect or other person
- Coroners, medical examiners and funeral directors
- Organ procurement organizations
- Avert a serious threat to health or safety
- Correctional institutions regarding inmates
- As authorized by state worker's compensation laws
- To the military, to federal officials for lawful intelligence, counterintelligence, and national security activities, and to correctional institutions and law enforcement regarding persons in lawful custody

Uses and Disclosures Requiring Your Written Authorization

Use or Disclosure with Your Authorization: For any purpose other than the ones described above, your PHI may be used or disclosed only when you provide your written authorization on an approved authorization form ("Authorization to Disclose Information"). For example, you will need to execute an authorization form before your PHI can be sent to your life insurance company or to the attorney representing the other party to litigation in which you are involved.

Marketing: We will not use your medical information for marketing purposes without your authorization. If you have consented to receive marketing information but no longer wish to receive further information, please call 1-877-367-5681 to make your opt-out request.

Special Privacy Protections for Alcohol and Drug Abuse

Information: Alcohol and drug abuse information has special privacy protections. We will not disclose any information identifying an individual as being a patient or provide any health information relating to the patient's substance abuse treatment unless the patient consents in writing; a court order requires disclosure of the information; medical personnel need the information to meet a medical emergency; qualified personnel use the information for the purpose of conducting scientific research, management audits, financial audits, or program evaluation; or it is necessary to report a crime or a threat to commit a crime, or to report abuse or neglect as required by law.

Your Rights Regarding Health Information About You

Right to Inspect and Copy: You have the right to inspect and copy information in your medical record. This right does not extend to any psychotherapy notes. To inspect and/or get a copy of your medical record you must submit your request in writing to the Medical Records department at the applicable Affiliated Entity. You may be required to pay copying costs.

Right to Amend: If you feel that information about you is incorrect, you may ask us to amend the record. To request an amendment, the request must be made in writing to the Medical Records department at the applicable Affiliated Entity. In addition, you must provide a reason that supports your request. We are not obligated to comply with your request to amend your record.

Right to Request Restrictions: You have the right to request limits on the use of your medical information for either treatment, payment or health care operations. You also have the right to request a limit on medical information we disclose to someone who is involved in your care or the payment of your care such as a family member or friend. For example, you could ask that we not disclose information about a surgery you had. To request restrictions, the request must be made in writing to the Medical Records department at the applicable Affiliated Entity. We are not required to agree to your request. If we do agree we will comply with your restrictions unless the information is needed to provide emergency treatment.

Right to Request Confidential Communications: You have the right to request that we communicate with you about medical matters in a certain way or at a certain location. For example, you can ask that we only contact you at work or by mail. Your request must specify how or where you wish to be contacted. We will accommodate all reasonable requests. To request restrictions, the request must be made in writing to the Medical Records department at the applicable Affiliated Entity.

Right to Revoke your Authorization: If you provide us with authorization to use or disclose medical information about you, you may revoke that authorization, in writing, at any time. If you revoke your authorization, we will no longer use or disclose medical information about you for the reasons covered by your written authorization. We are unable to take back any disclosures we have already made with your permission and we are required to retain our records of the care that we provided to you. A form of written revocation is available upon request from the Affiliated Entity's Medical Records Department.

Right to a Paper Copy of this Notice: If you view this Notice on our Web site or by electronic mail (e-mail), you are entitled to receive a copy of this Notice in written form. Please contact us as directed below to obtain this Notice in written form.

Breach Notification: In certain instances, you have the right to be notified in the event that we, or one of our Business Associates, discover an inappropriate use or disclosure of your health information. Notice of any such use or disclosure will be made in accordance with state and federal requirements.

Disposal of Medical Records: You have the right to know that your medical records may be destroyed ten (10) years after you were last treated in the hospital or, if you were younger than eighteen (18) years of age when you were last treated at the hospital, on your 20th birthday or on or ten (10) years after the date you were last treated, whichever date is later. St. Joseph may not destroy medical records that relate to any matter that is involved in litigation if St. Joseph knows the litigation has not been finally resolved. Such records may be destroyed upon final resolution of the litigation.

Right to an Accounting of Disclosures: You have the right to request an "accounting of disclosures." This is a list of disclosures that we have made about you. To request an accounting, the request must be made in writing to the Medical Records department at the applicable Affiliated

Entity. Certain time restrictions apply to a request for accounting of disclosures as well as the specification of the method for receiving the information.

Safeguards

St. Joseph safeguards customer information using various tools such as firewalls, passwords and data encryption. We continually strive to improve these tools to meet or exceed industry standards. We also limit access to your information to protect against its unauthorized use. The only St. Joseph workforce members who have access to your information are those who need it as part of their job. These safeguards help us meet both federal and state requirements to protect your personal health information.

St. Joseph Compliance and Privacy Office: If you would like more information about our privacy practices or have questions or concerns about this Notice, please contact the Compliance and Privacy Office at the number listed below.

If you believe your privacy rights have been violated, you may file a complaint, in writing, to the St. Joseph Health System Compliance and Privacy Office located at:
2801 Franciscan Drive, Bryan, Texas 77802
or by calling 979-776-5316, or you may contact the U.S. Department of Health and Human Services (DHHS)
1301 Young Street, Suite 1169
Dallas, TX 75202
Voice Phone 214-767-4056
FAX 214-767-0432
TDD 214-767-8940

To e-mail the DHHS Secretary or other Department Officials, send your message to hhs@mail@os.dhhs.gov

Affiliated Facilities/Entities

This Notice applies to the privacy practices of the following St. Joseph Health System Affiliated Entities which, for purposes of the Privacy Rule, hereby designate themselves as an organized health care arrangement:

St. Joseph Regional Health Center
St. Joseph Somerville Family Medicine
St. Joseph Caldwell Family Medicine Clinic
St. Joseph Lexington Family Medical Clinic
St. Joseph Franklin Family Medicine Clinic
St. Joseph Normangee Family Medicine
St. Joseph Family Medicine Madisonville
St. Joseph Hearne Family Medicine Clinic
J.B. Heath Family Health Center
Burleson St. Joseph Health Center
Grimes St. Joseph Health Center
Madison St. Joseph Health Center
St. Joseph Manor
Burleson St. Joseph Manor
St. Joseph Physician Associates

Acknowledgement of Notice of Privacy Practices

I acknowledge that I have received a copy of the Notice of Privacy Practices of the St. Joseph Health System, Bryan, Texas.

Signature of Patient or Authorized Representative

Date