IN THE SUPERIOR COURT OF THE STATE OF WASHINGTON
IN AND FOR THE COUNTY OF KING

STACY EDWARDS, individually and on behalf of all other similarly situated, S.A., individually and all those similarly situated, and JANE AND JOHN DOES 1-10, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

UNIVERSITY OF WASHINGTON,

Defendant.

Case No. 19-2-12285-4

THIRD AMENDED CLASS ACTION COMPLAINT

Plaintiffs Stacy Edwards, and S.A., individually and on behalf of the proposed Class defined below, brings this Class Action Complaint against Defendant University of Washington ("UW Medicine" or "Defendant"), and alleges as follows based on personal experience, information and belief, including investigation conducted by their undersigned attorneys:

I. NATURE OF THE ACTION

1. Plaintiffs bring this class action against UW Medicine for its failure to properly secure and safeguard the PHI of approximately 974,000 patients, including without limitation, patient names, medical record numbers, and other healthcare data, and for failing to provide timely, accurate, and adequate notice to Plaintiffs and the Class that the confidentiality of their

CORR CRONIN LLP
1001 Fourth Avenue, Suite 3900
Seattle, Washington 98154-1051
Tel (206) 625-8600
Fax (206) 625-0900

information had been breached. Plaintiffs seek, among other things, orders requiring UW Medicine to fully and accurately disclose the precise nature of data that has been compromised and to adopt reasonably sufficient security practices and safeguards to prevent incidents like the one described herein occurring in the future.

2. UW Medicine is one of the largest comprehensive, integrated healthcare providers in Washington State, providing medical care to patients around the globe. UW Medicine offers a variety of primary, specialty, urgent or emergent care, and air medical transport services to over 1.3 million patients per year at more than 300 locations around the Puget Sound region. UW Medicine's annual revenues in 2018 exceeded $5 billion. UW Medicine projects its revenues to reach over $5.3 billion for fiscal year 2019.

3. As one of the largest healthcare providers in Washington, UW Medicine collects, stores, and maintains a massive amount of PHI and other healthcare data on its patients, who are primarily Washington state residents, and who entrust their information to UW Medicine with the expectation that UW Medicine will exercise due care in protecting such information. At all relevant times, Plaintiffs and the Class have taken reasonable steps to protect their PHI, including relying upon the physician-patient privilege and UW Medicine's representations about maintaining the confidentiality of their information.

4. UW Medicine is required to protect patient information, including by adopting and implementing specific data security practices, policies, and procedures required under Washington's Health Care Information Act, Washington's Omnibus AIDS Act, and the federal Health Insurance Portability and Accountability Act of 1996. Healthcare data used for research purposes is also regulated by Washington's Release of Records for Research Act.

5. In addition to these express statutory duties, UW Medicine assumed other legal, equitable, and contractual duties to Plaintiffs and the Class in connection with obtaining, collecting, storing, using, creating, and transmitting Plaintiffs and the Class' healthcare data and

CORR CRONIN LLP
1001 Fourth Avenue, Suite 3900
Seattle, Washington 98154-1051
Tel (206) 625-8600
Fax (206) 625-0900

PHI. UW Medicine knew or should have known that it was responsible for protecting Plaintiffs and the Class' PHI from disclosure, exposure, and/or unauthorized use or access. Indeed, UW Medicine promised Plaintiffs and the Class that it would protect their data from unauthorized exposure, disclosure, use, or access.

6. Unfortunately, UW Medicine's failure to protect its patients' data resulted in one of the largest, if not the largest, known breaches of PHI by a public medical system in state history.

7. On or about February 20, 2019, UW Medicine revealed that, due to human error, files containing PHI and other healthcare data of approximately 974,000 patients were compromised and freely accessible on the internet from approximately December 4, 2018 to approximately January 10, 2019 (the "Breach"). According to UW Medicine, the exposure included the PHI of unsuspecting patients who treated at UW Medicine and disclosed their information in trust and confidence, and in reliance, in part, on UW Medicine's representations and promises that it would exercise due care in protecting their healthcare data and/or PHI.

8. According to UW Medicine, it first learned of the Breach on December 26, 2018, but waited almost two months to disclose the Breach to the public and individuals known to have been impacted by the Breach in violation of Washington state law.

9. The Breach not only revealed that UW Medicine failed to provide the level of data protection it promised and that its patients paid for, but this was not the first time UW Medicine has exposed the PHI of its patients due to inadequate information security practices. In 2013, UW Medicine exposed the PHI and, in some instances social security numbers, of 90,000 patients after an employee opened an attachment containing malware. In December 2015, UW Medicine settled charges brought by the U.S. Department of Health and Human Services ("HHS"), which claimed that UW Medicine violated the HIPAA Security Rule by failing to implement adequate policies and procedures to prevent, detect, contain, and correct

CORR CRONIN LLP
1001 Fourth Avenue, Suite 3900
Seattle, Washington 98154-1051
Tel (206) 625-8600
Fax (206) 625-0900

data security violations. In addition to paying $750,000 to settle the charges, UW Medicine promised HHS that it would conduct a comprehensive risk analysis of security risks and vulnerabilities and develop an organization-wide risk management plan. The Breach at the heart of this case occurred just three years later.

10. UW Medicine clearly failed to institute all measures it needed to after the 2013 data breach to ensure that the healthcare data was adequately protected. Its substandard security practices have now compromised nearly one million patients' PHI, greatly exceeding the scope of the 2013 breach, in violation of its statutory and professional standard of care obligations, in breach of Plaintiffs and the Class' reasonable expectations when they decided to form a patient-physician relationship with UW Medicine, and thereby diminishing the value of the services UW Medicine provided and that its patients paid for.

II. PARTIES TO THE ACTION

11. Plaintiff Stacy Edwards is a natural person and a Washington resident, residing in King County, Washington. Ms. Edwards brings this action on behalf of herself and the proposed Class defined below. Ms. Edwards delivered her only child at UW Medicine, in addition to attending a sleep clinic at Harborview Medical Center from 2015 through 2017. Prior to electing to treat at UW Medicine, she entered into contracts with UW Medicine for healthcare services in exchange for money under which UW Medicine agreed in part to protect her healthcare data, and thereby assumed a contractual and legal duty to do the same. She discovered that her PHI had been compromised as a result of UW Medicine's actions in or about February 2019. UW Medicine has not disclosed all of the facts of the breach to Ms. Edwards. Like all affected individuals, Ms. Edwards entered into a contract and patient-physician relationship with UW Medicine and paid money to UW Medicine based in part on UW Medicine's promise to properly safeguard her healthcare data. Ms. Edwards has been and is being damaged as a result of the Breach in an amount to be proven at trial. She has spent time

CORR CRONIN LLP
1001 Fourth Avenue, Suite 3900
Seattle, Washington 98154-1051
Tel (206) 625-8600
Fax (206) 625-0900

and energy responding to the Breach. She purchased medical identity theft and credit monitoring services as a result of the Breach. She complied with Washington State's notice of claim statute before filing this action.

12. Plaintiff S.A. is a natural person and a Washington resident, residing in King County, Washington. S.A. brings this action on behalf of himself and the proposed Class defined below. Prior to receiving care at UW Medicine, he entered into a contract for healthcare services in exchange for money, under which UW Medicine agreed in part to protect his healthcare data, and thereby assumed a contractual and legal duty to do the same. Like all affected individuals, S.A. entered into a contract and patient-physician relationship with UW Medicine and paid money to UW Medicine based in part on UW Medicine's promise to properly safeguard his healthcare data. In or about February 2019, S.A. discovered that his PHI and other healthcare data, including information regarding sensitive lab tests, had been unlawfully disclosed by UW Medicine as a result of human error. S.A. has been and is being damaged as a result of the Breach in an amount to be proven at trial. He has spent time and energy responding to the Breach. He complied with Washington State's notice of claim statute before filing this action.

13. Plaintiffs reserve the right to add additional Jane and John Does, who, like Ms. Edwards and S.A., have been harmed by UW Medicine.

14. Defendant University of Washington owns and operates UW Medicine, which consists of the following component entities: University of Washington Medical Center, University of Washington School of Medicine, Harborview Medical Center, Valley Medical Center, UW Medicine Neighborhood Clinics, Northwest Hospital, and UW Physicians Network d/b/a UW Neighborhood Clinics, and Airlift Northwest, and the University of Washington's membership in Children's University Medical Group, and Seattle Cancer Care Alliance. Defendant University of Washington is a public university based in King County, Washington.

CORR CRONIN LLP
1001 Fourth Avenue, Suite 3900
Seattle, Washington 98154-1051
Tel (206) 625-8600
Fax (206) 625-0900

III. JURISDICTION AND VENUE

15. This Court has subject matter and personal jurisdiction under Washington law.

16. Venue is also proper because Defendant is based in and conducts business in King County, Washington.

17. Federal jurisdiction is precluded under the Class Action Fairness Act ("CAFA") under 28 U.S.C. § 1332(d)(5), which excludes from CAFA's scope "any class action in which *** the primary defendants are States, State officials, or other government entities ***." Because the primary, indeed the only, defendant in this case is the University of Washington, federal jurisdiction is precluded under § 1332(d)(5).

IV. FACTS

A. UW Medicine's Insufficient Data-Security Practices Compromised the PHI of Nearly One Million Patients

18. Based on obligations created under common law, state and federal statutes, and industry standards, among other sources, UW Medicine owed duties to Plaintiffs and the Class to adopt and maintain sufficient security measures to secure and safeguard their PHI and other healthcare data.

Based on Plaintiffs' investigation and discovery completed to date, UW Medicine indisputably breached these duties by failing to adopt and maintain adequate security measures and by compromising the healthcare information and/or PHI of nearly one million patients.

19. In a press release issued on February 20, 2019, UW Medicine admitted that it compromised the PHI of approximately 974,000 patients due to internal human error:

> On Dec. 26, 2018, UW Medicine became aware of a vulnerability on a website server that made protected internal files available and visible by search on the internet on Dec. 4, 2018. The files contained protected health information (PHI) about reporting that UW Medicine is legally required to track, such as reporting to various regulatory bodies, in compliance with Washington state reporting requirements.

CORR CRONIN LLP
1001 Fourth Avenue, Suite 3900
Seattle, Washington 98154-1051
Tel (206) 625-8600
Fax (206) 625-0900

> ****
>
> Based on the results of our internal investigation, we are in the process of distributing letters to approximately 974,000 affected patients and have reported this incident to the Office for Civil Rights.
>
> ****
>
> The files became accessible on December 4, 2018 due to an internal human error. UW Medicine fixed the error immediately upon discovery on December 26, 2018. Because Google had saved some of the files before December 26, 2018, UW Medicine worked with Google to remove the saved versions and prevent them from showing up in search results. All saved files were completely removed from Google's servers by January 10, 2019.

20. While UW Medicine's press release provided very little specifics on the type of data disclosed, the online version included a question and answer section, which added that the database subject to exposure was used to track instances where UW Medicine shares protected health information with other providers or authorities, or where such information is accessed by research professionals:

> The database is used to keep track of the times UW Medicine shares patient health information that meets certain legal criteria. UW Medicine is required to track this information by the HIPAA law, which is overseen by the Office for Civil Rights.
>
> The most common reasons involve situations where UW Medicine is required by Washington state law to share patient information with public health authorities, law enforcement and Child Protective Services.
>
> Another common example is when a researcher receives approval to access medical records to determine whether a patient may be eligible for a research study or to recruit participants. The researcher must document in the database when they access the medical record.[1]

21. The question and answer section further explained that UW Medicine discovered the Breach after a patient accessed the database after conducting a Google search for their own name:

[1] *Data Error Exposes Patient Information*, UW Medicine Newsroom, accessible at https://newsroom.uw.edu/news/data-error-exposes-patient-information.

CORR CRONIN LLP
1001 Fourth Avenue, Suite 3900
Seattle, Washington 98154-1051
Tel (206) 625-8600
Fax (206) 625-0900

> UW Medicine became aware of this incident on December 26, 2018, when a patient was conducting a Google search for their own name and found a file containing their information. The patient reported this to UW Medicine.

22. Shortly after the public learned of the Breach, local news outlets reported that the database had been accessed by other third parties, and that the exposed data included patient information related to HIV:

> Meagan Flory told KIRO 7 she accessed some of the UW Medicine files through a Google search last month after a friend discovered the exposed personal information when looking up a person's name she'd met.
>
> "Upset about something she'd stumbled across online," said Flory. "It clearly said it was UW Medicine."
>
> Flory said there were as many as 120 names in the UW Medicine she accessed through a Google search that also included the names of those patient's lab tests but not the results.
>
> "HIV was one of them?" asked KIRO 7 report Michael Spears.
>
> "That was what they all were, pretty much," said Flory.
>
> ****
>
> "Having this out on Google like that is scary," said Flory. "You know it could be upsetting or devastating for somebody."

23. Through discovery in this case, Plaintiffs have learned that the database entries exposed online refer to the individual as a patient of UW Medicine and contain, in addition to the patient's name and medical record number, (a) descriptions of the PHI disclosed to researchers, including identification of the nature of the records (e.g. "ICU flow sheets") and/or the medical department (e.g. "cardiology") from which the PHI was disclosed, and/or (b) information about the research studies themselves, including the names of the researchers and their institutional affiliations. Further, UW Medicine acknowledged in its press release that the database contained individually identifiable information relating to the health status of patients of UW Medicine, such as diagnoses and treatment information (e.g. that a patient took an HIV test, was treated in the cardiology department, or underwent intensive care in the ICU). The

CORR CRONIN LLP
1001 Fourth Avenue, Suite 3900
Seattle, Washington 98154-1051
Tel (206) 625-8600
Fax (206) 625-0900

following is a rough illustration of the type of data that was unlawfully disclosed and how the information appeared to the world online:

Patient No./MRN	Patient Last Name	Patient First Name	Patient Middle Name	Date of Disclosure	Contact Information of the entity or person who received the PHI	Brief Description of the PHI disclosed
N/A	N/A	N/A	N/A	N/A	N/A	N/A

24. Discovery has also corroborated reporting by KIRO 7 shortly after the public learned of the Breach that the exposed data also included patient-HIV information. Through discovery and public record requests, Plaintiffs have confirmed that the exposed information included information reflecting a patient's HIV test-taking history and even status, along with medical record numbers, names, and other sensitive patient-accounting information. Moreover, discovery has confirmed that at the time it notified the victims and the public about the Breach, it knew that the exposed database had been accessed by unauthorized parties but told the victims and the public that there was nothing to worry about and no evidence of harm. UW Medicine blatantly mislead the victims and the public about the Breach by omitting these and other material facts. The only reasonable explanation for such unscrupulous behavior is that UW Medicine wanted to paint a rosier picture than was actually the case to mitigate both the public fall-out and potential for future liability. In doing so, UW Medicine and, by extension the State of Washington, violated its duties of trust and confidence to its patients, and its position of trust in relation to the public at large given its status as a public entity. UW Medicine disappointingly acted just like any corporate entity in the throes of a crisis: it looked out for its bottom line.

CORR CRONIN LLP
1001 Fourth Avenue, Suite 3900
Seattle, Washington 98154-1051
Tel (206) 625-8600
Fax (206) 625-0900

25. The Breach occurred because UW Medicine failed to adopt, maintain, and carry out adequate information security practices, protocols, and policies. In so doing, UW Medicine failed to fulfill its duties and promises to its patients to (i) take sufficient precautions and implement sufficient policies and practices necessary to safeguard patient healthcare data; (ii) obtain patient consent before disclosing or exposing patient PHI on the internet; (iii) detect and address system vulnerabilities and secure its systems from misconfiguration resulting in unauthorized access or exposure; (iv) enforce or monitor employee compliance with good practices, industry standards and/or state or federal laws or regulations; and (v) timely and reasonably notify affected patients that their data had been compromised. As one veteran chief technology officer observed in a Forbes article published just a few months after the Breach, UW Medicine's exposure of nearly 1 million patients' PHI was definitely due to either "ignorance or negligence."[2]

26. Among other statutory regimes, Washington's Uniform Healthcare Information Act, Washington's Omnibus AIDS Act, and the federal Health Insurance Portability and Accountability Act of 1996 regulate UW Medicine's storage, use, creation, transmission, custody, protection, and disclosure of healthcare data. Among other things, these statutes require UW Medicine to properly safeguard the privacy of applicable patient information and to promptly notify patients of any breach.

27. UW Medicine also explicitly promises patients that it will safeguard their PHI. In its Joint Notice of Privacy form, which UW Medicine posts on its website and gives to all new patients, UW Medicine promises to safeguard the privacy of patient information and to promptly notify patients of any breach:

[2] *It's Time to Put a Stop to Security Breaches Caused by Human Error,* Forbes Technology Council, accessible at https://www.forbes.com/sites/forbestechcouncil/2019/05/29/its-time-to-put-a-stop-to-security-breaches-caused-by-human-error/#6fe9591f17d4.

CORR CRONIN LLP
1001 Fourth Avenue, Suite 3900
Seattle, Washington 98154-1051
Tel (206) 625-8600
Fax (206) 625-0900

OUR RESPONSIBILITIES

- We are required by law to maintain the privacy and security of your protected health information.
- We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information.
- We must follow the duties and privacy practices described in this notice and give you a copy of it.
- We will not use or share your information other than as described here unless you tell us we can in writing. If you tell us we can, you may change your mind at any time. Let us know in writing if you change your mind.[3]

28. In its Notice of Privacy Practices Acknowledgement Form, which all patients must sign to acknowledge receipt of the Joint Notice of Privacy Form, UW Medicine confirms: "We have a responsibility to protect the privacy of your information, provide a Notice of Privacy Practices, and follow the information practices that are described in this notice."[4]

29. UW Medicine's Compliance Policies pertaining to patient information further define the broad contours of its duties and promises to appropriately safeguard healthcare data. For example, UW Medicine's Compliance Policy 102, which it posts on its website, promises patients the following:

> **Safeguarding the Privacy and Security of Protected Health Information (PHI)**
>
> UW Medicine safeguards the confidentiality, integrity and availability of PHI in all forms (including verbal, paper and electronic) and in all locations. UW Medicine uses a role-based model to identify appropriate levels of access to PHI.
>
> UW Medicine workforce members are personally and professionally responsible for appropriately protecting PHI to which they are given access. For example, workforce members must only discuss patient information in the appropriate workplace setting, and only with those who have a need-to-know and the authority to receive the information. Workforce members must keep paper-based patient information out of view of patients, visitors and workforce members who

[3] *Joint Notice of Privacy Practices*, UW Medicine, accessible at http://depts.washington.edu/comply/docs/104_F2.pdf. An example is attached hereto.

[4] *Notice of Privacy Practices Acknowledgment Form*, UW Medicine, accessible at http://depts.washington.edu/comply/docs/104f9_NPriAck.pdf. An example is attached hereto.

CORR CRONIN LLP
1001 Fourth Avenue, Suite 3900
Seattle, Washington 98154-1051
Tel (206) 625-8600
Fax (206) 625-0900

> are not involved in the patient's care, and dispose of it in a secure and confidential manner. Patient information taken off-site must be kept fully secured, remain in the workforce member's physical possession during transit, never be left unattended and never be left in any mode of transport (even if it is locked).
>
> UW Medicine verifies the identity of all requestors and the requestors' legal authority for obtaining PHI. For disclosures made on a routine or recurring basis, UW Medicine departments implement policies and procedures that limit the PHI disclosed to the amount reasonably necessary to achieve the purpose of the disclosure.

30. UW Medicine's Compliance Policy 103, which it also posts on its website, promises patients in part that it will adhere to the "Minimum Necessary" principle in using or disclosing their PHI:

> **The Minimum Necessary Requirement**
>
> UW Medicine takes reasonable precautions to ensure that uses of, disclosures of, or requests for PHI are limited to the minimum necessary. Minimum necessary is based on a need-to-know and is the limited PHI required to accomplish the intended purpose of the use or disclosure or request. UW Medicine shall not use, disclose or request an entire medical record from another covered entity unless access to the entire medical record is specifically justified as the amount of information reasonably necessary to accomplish the purpose of the request.

31. By including these and other policies and statements on its website concerning the steps it promises patients it will take to safeguard their information, and by requiring patients to acknowledge their understanding of its privacy policies prior to receiving treatment, UW Medicine clearly recognized the importance of safeguarding patient healthcare data from unauthorized access, use, or disclosure, and expressly promised its patients that it would safeguard such information. Plaintiffs relied on the promises therein in choosing to obtain healthcare from UW Medicine.

32. UW Medicine's failure to fulfill its duties and promises to safeguard healthcare data take on increased urgency in light of the fact that this was not the first time UW Medicine has breached the confidentiality of patient information due to inadequate information security practices.

CORR CRONIN LLP
1001 Fourth Avenue, Suite 3900
Seattle, Washington 98154-1051
Tel (206) 625-8600
Fax (206) 625-0900

33. Specifically, in November 2013, UW Medicine compromised the PHI of 90,000 patients after an employee opened an email attachment containing malicious software. After reporting the incident to the FBI, the U.S. Department of Health and Human Services, Office for Civil Rights, brought charges against UW Medicine for violation of the HIPAA Security Rule by failing to implement adequate policies and procedures to prevent, detect, contain, and correct data security violations. UW Medicine settled these charges in December 2015. In addition to paying $750,000, UW Medicine agreed to take corrective actions including: (1) developing a comprehensive risk analysis and management program to address risks and vulnerabilities to electronic protected health information (e-PHI) created, received, maintained or transmitted by UW Medicine; (2) conducting annual audits to assess the adequacy of its risk management program to protect e-PHI, to mitigate risks to e-PHI, and update its policies and procedures with additional security measures as needed; and (3) periodic compliance reporting to HHS regarding the implementation of its risk management program and any HIPAA Security Rule violations should they occur.

34. Despite settling HHS' charges related to the 2013 incident, UW Medicine's breach in this case shows that it failed to implement and maintain adequate security measures to prevent, detect, contain, and correct security risks and safeguard PHI. Among other things, the fact that UW Medicine published the PHI of approximately 974,000 patients on the internet due to internal human error means that they failed to maintain adequate security, storage, transmission, and handling processes and protocols in order to property safeguard patient information; failed to ensure the confidentiality and integrity of the healthcare data it created, received, maintained, and transmitted in the course of UW Medicine's operations; failed to protect against reasonably anticipated or foreseeable threats or hazards to the security or integrity of patient information; failed to ensure compliance with Washington state and HIPAA security standards by its workforce; failed to train all members of its workforce on the policies

CORR CRONIN LLP
1001 Fourth Avenue, Suite 3900
Seattle, Washington 98154-1051
Tel (206) 625-8600
Fax (206) 625-0900

and procedures as necessary to carry out their functions while maintaining the security of protected health information; and failed to reasonably and promptly notify all affected patients and provide them with the information they need to protect themselves.

35. As UW Medicine wrongfully exposed and disseminated Plaintiffs and the Class' healthcare data into the public domain in violation of UW Medicine's duties and promises to safeguard the confidentiality of such information, Plaintiffs and the Class have undeniable interest in ensuring that UW Medicine adopt appropriate safeguards that their health information is protected and will remain protected in the future. Plaintiffs thus bring this action against UW Medicine to vindicate the rights and privacy interests of themselves and the 974,000 other patients who were harmed by the Breach; and to guarantee that UW Medicine adopts sufficient safeguards to ensure something like this, and, for that matter, the 2013 breach, never happens again.

B. Plaintiffs and the Class Have Suffered Real, Significant, and Continuing Injury

36. Data-breach victims, such as Plaintiffs and the Class here, experience real, significant, and continuing injury.

37. It is an established fact that the harms caused by involuntary disclosure of personal information are continuing and the consequences of a breach can follow the affected individuals for a lifetime. The Federal Trade Commission estimates that over 15 million people experience identity theft every year in the United States. A 2014 report by the U.S. Department of Justice found that victims of identity theft suffer average individual losses of $1,343.[5] According to Javelin Strategy and Research, one in four data-breach victims experience identity theft.[6] Further, once a victim's information has been compromised, criminals often trade the

[5] *Victims of Identity Theft, 2014*, DOJ Publication, accessible at www.bjs.gov/content/pub/pdf/vit14.pdf.

[6] *2013 Identity Fraud Report: Data Breaches Becoming Treasure Trove for Fraudsters*, accessible at https://www.javelinstrategy.com/coverage-area/2013-identity-fraud-report-data-breaches-becoming-treasure-trove-fraudsters.

CORR CRONIN LLP
1001 Fourth Avenue, Suite 3900
Seattle, Washington 98154-1051
Tel (206) 625-8600
Fax (206) 625-0900

information on the black market for years. As the FTC has recognized, data criminals are increasingly combining disparate pieces of data from multiple sources to perpetrate identity crimes that often take years to fully materialize.[7]

38. Compromised personal information exposes victims to loss of reputation, loss of employment, blackmail and other negative effects such as incarceration. [8] Victims are forced to spend countless hours and large amounts of money repairing the impact to their credit and personal lives. The United States Government Accountability Office has found that victims of identity crimes face "substantial costs and inconveniences repairing damage to their credit records" and their "good name."[9]

39. Victims of medical identity theft, in particular, face severe and potentially catastrophic social, financial, and economic injuries. Medical identity theft – or the misuse of another person's individual identifying medical information – has been identified as one of the fastest growing crimes in America. According to the Ponemon Institute, medical identity theft results in over $30 billion in costs per year and victims pay on average $13,500 to address the harms caused by the crime.[10] There is a well-established and lucrative black market for healthcare information, including data obtained from misconfigured websites.[11] Stolen

[7] Protecting Consumer Privacy in an Era of Rapid Change – March 2012, FTC Report, accessible at https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[8] *See Remsburg v. Docusearch, Inc.*, 149 N.H. 148, 816 A.2d 1001, 1008 (N.H. 2003) ("[Identity theft] often destroys a victim's ability to obtain credit from any source and may, in some cases, render the victim unemployable or even cause the victim to be incarcerated.").

[9] *Data Breaches and Identity Theft*, GAO-07-737, accessible at http://www.gao.gov/new.items/d07737.pdf.

[10] *See Fifth Annual Study on Medical Identity Theft*, Ponemon Institute, accessible at http://www.medidfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_Theft_Study1.pdf.

[11] *See, e.g., Healthcare Hack: PHI For Sale on DarkNet*, HIPAA for MSPs, accessible at https://www.hipaaformsps.com/healthcare-hack-phi-for-sale-on-the-darknet/.

CORR CRONIN LLP
1001 Fourth Avenue, Suite 3900
Seattle, Washington 98154-1051
Tel (206) 625-8600
Fax (206) 625-0900

healthcare information can reportedly sell for up to $350 or $500 per record.[12] Further, ePHI and healthcare data has a longer shelf life than credit card information or other forms of PHI and thus can be used for more sophisticated, lucrative, and successful campaigns.

40. Third parties harvest personal information through intrusive hacking attempts or simply by using Google or software downloadable online to scour the internet for unsecured and/or misconfigured databases.[13] Misconfigured and/or unsecured databases, like the one at issue here, plague the healthcare sector at alarming rates. A recent study published by the cyber-intelligence firm IntSights found that approximately 30% of the healthcare databases it found on the internet were misconfigured and freely accessible to the public. The researchers accessed over 1.5 million exposed healthcare records after just 90 hours of research, at a rate of 16,667 records per hour. Based on these figures, IntSights calculated that third parties who harvest data from exposed databases and sell the information on the black market could earn an annual salary of $33 million per year working just a standard, 40-hour workweek. The researchers cautioned that "[w]ith simple search techniques and a basic understanding of how these systems work, you can find an endless amount of ePHI data" online.[14]

41. Besides the financial burden posed on patients, hospitals, insurance companies, and government insurance programs alike, compromised medical information poses major quality-control and safety risks to patients and providers. While Plaintiffs anticipate UW Medicine to argue that Plaintiffs and the Class have not been harmed, this is not so. Aside from

---

[12] *See Data Breaches: In the Healthcare Sector*, Center for Internet Security, accessible at https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/. *See also Hackers Selling Healthcare Data in the Black Market*, InfoSec, accessible at https://resources.infosecinstitute.com/hackers-selling-healthcare-data-in-the-black-market/#gref.

[13] *Your Most Sensitive Data is Likely Exposed Online. These People Try to Find It*, CNET, accessible at https://www.cnet.com/news/your-most-sensitive-data-is-likely-exposed-online-these-people-try-to-find-it/.

[14] *Exposed & Misconfigured Databases in the Healthcare Industry*, IntSights, accessible at https://intsights.com/resources/chronic-cyber-pain-exposed-misconfigured-databases-in-the-healthcare-industry.

CORR CRONIN LLP
1001 Fourth Avenue, Suite 3900
Seattle, Washington 98154-1051
Tel (206) 625-8600
Fax (206) 625-0900

the breach of contract and deprivation of privacy and statutory rights caused by the Breach – which constitute immediate, continuing, and cognizable injuries in and of themselves – the type of data compromised in this case can be used by unauthorized third parties to access and misappropriate a patient's medical history and can lead to misdiagnosis and/or erroneous treatment causing serious injury or death.

42. Medical record numbers (MRNs), in particular, serve as a critical link between a patient and their medical history. Healthcare providers use MRNs to track systematically a patient's medical history and treatment from the inception of the physician-patient relationship. As a result, compromised MRNs threaten everything from the integrity of a provider's billing and recordkeeping system to, more importantly, the patient's privacy and physical safety. For example, a case of compromised MRNs recently resulted in a Worcester, Massachusetts hospital's mistaken surgical removal of a healthy patient's kidney.[15] A 2014 report by the Joint Commission Journal on Quality and Patient Safety found at one major hospital that at least 14 patients each year were treated under the wrong medical record number, and an estimated 25 patient encounters each quarter were tied to medical identity theft or fraud.[16] Experience also shows that MRNs paired with other personally identifiable information such as a name can be used by third parties to obtain unauthorized access to a person's medical history. In one example, a woman posted her story online of how her ex-husband obtained her medical records illegally from one of her providers using her medical record number, and then submitted the misappropriated records as evidence against her in their divorce proceedings. Given the importance of MRNs to hospital systems, and the ability to use MRNs to access a treasure-trove

[15] *Faulty ID Methods Led to Surgical Error at St. Vincent Hospital*, Worcester Telegram & Gazette, accessible at https://www.telegram.com/news/20161013/faulty-id-methods-led-to-surgical-error-at-st-vincent-hospital.

[16] *Medical Identity Theft: Prevention and Reconciliation Initiatives at Massachusetts General Hospital*, Jt. Comm. J. Qual. Patient Saf., accessible at https://www.ncbi.nlm.nih.gov/pubmed/25130011.

CORR CRONIN LLP
1001 Fourth Avenue, Suite 3900
Seattle, Washington 98154-1051
Tel (206) 625-8600
Fax (206) 625-0900

of information about a particular patient, it is no surprise that there have been repeated instances of hackers targeting hospitals with malicious software[17] and online phishing attacks[18] to obtain such information. Compounding the problem, given the nature of the crime, the harms victims of medical identity theft experience take months if not years to fully materialize. Unfortunately, by the time the victim learns the full extent of harm or that their identity has been compromised the consequences can be devastating. A 2012 report by the Healthcare Information and Management Systems Society recounts the story of a woman whose medical identity was sold on the black market and who almost lost custody of her four children after the person who purchased her data gave birth to a drug-addicted baby. The same report tells the story of another woman who received a hospital bill for amputation of her right foot even though her foot had never been amputated. It was not until a year later, just before she was to undergo a hysterectomy, that she discovered the identity thief's medical information had become "intermingled" with her own after a nurse noted incorrectly that she had diabetes. "I now live in fear," the woman later explained, "that if something ever happened to me, I could get the wrong kind of medical treatment."[19]

43. Disclosure of healthcare information also causes significant social and reputational harms to its victims, due to the inherently personal and sensitive nature of such information. The disclosure patient-HIV test-taking history and HIV statuses is a vivid example of this harm. In a 2018 study on the effects of HIV-related stigma in the United States,

---

[17] *HAP, Blue Cross Blue Shield Customers' Information at Risk After Data Breach of Vendor*, Detroit Free Press, accessible at https://www.freep.com/story/news/local/michigan/2019/03/05/hap-data-breach/3067021002/.

[18] *See Cyber Criminals Target Cancer Patients in Possible Medical Data Breach*, WFLA, accessible at https://www.wfla.com/8-on-your-side/better-call-behnken/cyber-criminals-target-cancer-patients-in-possible-medical-data-breach/1640859489.

[19] *Creating a Trusted Environment; Reducing the Threat of Medical Identity Theft*, HIMSS Privacy & Security Task Force, accessible at https://risk.lexisnexis.com/cross-industry-fraud-files/docs/healthcare/Creating-Trusted-Environment-Reducing-Threat-Medical-Identify-Theft.pdf.

CORR CRONIN LLP
1001 Fourth Avenue, Suite 3900
Seattle, Washington 98154-1051
Tel (206) 625-8600
Fax (206) 625-0900

researchers noted the wide body of literature finding that such stigma causes persons to "lose social value and standing," and that it also has "negative effects on health outcomes, including ... higher depression[] and overall lower quality of life."[20] Indeed, even in Western countries in the 21st century, it is well established that "[t]he relatively specific sexual connotations associated with HIV infection, and its association with drug addiction, have meant that it is a highly stigmatized disease," and that such stigma "can result in marginalization, discrimination, and even physical hurt."[21] Notwithstanding the volumes of publically available information of the real and foreseeable harms done to data-breach victims, especially victims of healthcare related breaches, UW Medicine failed to properly safeguard Plaintiffs and the Class' protected health information, despite promising to do so. UW Medicine knew or should have known that the rate of data breaches in the healthcare sector has skyrocketed over the past decade and thus the threat posed to the confidentiality of Plaintiffs and the Class' healthcare information was greater than ever before. In fact, just a few months prior to the Breach, the Journal of the American Medical Association published a study showing that data breaches in the healthcare sector was a systemic problem.[22] The AMA study, published by researchers at the Massachusetts General Hospital Center for Quantitative Health, found that healthcare data breaches had increased a staggering 70% since 2010, with 75% of these records (or approximately 132 million records) being breached by an intentional hacking or IT-related loss, such as here. Moreover, the same study found that healthcare providers such as hospitals and clinics like UW Medicine have experienced the highest number of data breaches in the industry

[20] Bulent Turan et al., *How Does Stigma Affect People Living with HIV? The Mediating Roles of Internalized and Anticipated HIV Stigma in the Effects of Perceived Community Stigma on Health and Psychosocial Outcomes,* AIDS Behav. 2017 Jan.; 21(1): 283-291, accessible at https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5143223/.

[21] Mike Williams, *Confidentiality of the medical records of HIV-positive patients in the United Kingdom – a medicolegal and ethical perspective,* Risk Manag. Healthc. Policy, 2011, 4:15-26.

[22] *Temporal Trends and Characteristics of Reportable Health Data Breaches, 2010-17,* JAMA 320 (12), accessible at https://jamanetwork.com/journals/jama/fullarticle/2703327.

CORR CRONIN LLP
1001 Fourth Avenue, Suite 3900
Seattle, Washington 98154-1051
Tel (206) 625-8600
Fax (206) 625-0900

– *over 1,500*. Given these findings, one of the study's authors did not mince words when asked to summarize the takeaway from their research: "The reality is our patients have an expectation of confidentiality. These breaches are cases where we've failed to meet that expectation ***."[23]

44. Adding insult to injury, not only has UW Medicine recklessly and/or negligently failed to properly safeguard Plaintiffs and the Class' PHI, but UW Medicine has failed to offer sufficient relief to Plaintiffs and the Class that will make them whole and protect them from future harm. For instance, UW Medicine has elected not to offer Plaintiffs and the Class credit monitoring or identity-theft insurance that could help mitigate potential harms caused by the Breach, nor did UW Medicine disclose all material information about the Breach, forcing Plaintiff Edwards to purchase these services out of her own pocket to protect herself without knowledge of all of the underlying facts. UW Medicine's self-serving rationale for this decision is that there is no evidence the Breach caused any immediate injuries despite reams of publically available evidence and experience demonstrating that medical data-breach victims suffer not only immediate harms in the form of loss of privacy, deprivation of statutory rights, contract damages, and out-of-pocket costs responding to the breach, but also imminent, impending, and increased risk of future harms such as identity theft and/or fraud that often take years to fully materialize. No doubt Plaintiffs and the Class are incurring and will continue to incur damages due to UW Medicine's wrongful conduct and breach of its duties and promises, necessitating this lawsuit.

45. As a direct and proximate result of UW Medicine's wrongful action and inaction proximately and directly caused Plaintiffs and the Class to suffer and continue to suffer personal, social, economic, and financial losses, including without limitation:

a. exposure of their PHI;

[23] *Government Data Says Millions of Health Records Are Breached Every Year*, Forbes, accessible at https://www.forbes.com/sites/michelatindera/2018/09/25/government-data-says-millions-of-health-records-are-breached-every-year/#71ed8de516e6.

CORR CRONIN LLP
1001 Fourth Avenue, Suite 3900
Seattle, Washington 98154-1051
Tel (206) 625-8600
Fax (206) 625-0900

b. breach of contract and damages therefrom;

c. loss or invasion of privacy;

d. reputational loss and emotional distress;

e. deprivation of rights they possess under state and federal law;

f. imminent, impending, and increased risk of identity theft and/or healthcare fraud or abuse;

g. ascertainable losses in the form of out-of-pocket expenses, lost time responding to the breach, and deprivation of value of PHI;

h. statutory damages and penalties;

i. damages for restitution or unjust enrichment;

j. attorneys' fees and litigation costs; and

k. various other current, actual and/or imminent harms occurring now or reasonably certain to occur in the future.

46. UW Medicine owed Plaintiffs and the Class common law and statutory duties to protect their healthcare data, and it promised it would do so in connection with its physician-patient relationship with Plaintiffs and the Class. Plaintiffs and the Class paid UW Medicine money in reliance on its promises and representations that it would protect their healthcare data and PHI. As a result of UW Medicine's unlawful, and indeed wrongful, conduct described herein, Plaintiffs and the Class were deprived of the benefit of their bargain and now must spend years untangling the mess created by the Breach and mitigating the actual and potential harms caused by the Breach. The appropriate monetary, equitable, and injunctive relief owed by UW Medicine to Plaintiffs and the Class is ascertainable and should be determined at trial.

V. CLASS ACTION ALLEGATIONS

47. Plaintiffs seek relief in their individual capacities and as a representative of all others who are similarly situated. Pursuant to the Washington Civil Rules, Plaintiffs seek certification of a class consisting of all persons whose confidential information was

CORR CRONIN LLP
1001 Fourth Avenue, Suite 3900
Seattle, Washington 98154-1051
Tel (206) 625-8600
Fax (206) 625-0900

compromised in the Breach disclosed by UW Medicine on February 20, 2019. Alternatively, Plaintiffs seek the certification of a class consisting of all persons currently residing in the State of Washington whose information was compromised in the Breach disclosed by UW Medicine on February 20, 2019. Plaintiffs reserve the right to amend or supplement and seek subclasses depending on the facts revealed in discovery, including but not limited to individual classes and/or subclasses regarding Plaintiffs' claims under RCW 70.02 and RCW 70.24.

48. Excluded from the above Class is UW or UW Medicine, including any entity which UW has a controlling interest, as well as successors and assigns of UW. Also excluded are the judges, court personnel, and attorneys in the case and their immediate family members. Also excluded are potential members that opt out of the Class.

49. **Numerosity.** The members of the Class are so numerous that the joinder of all members is impractical. UW Medicine has acknowledged that the healthcare data and/or PHI of approximately 974,000 has been compromised in connection with the Breach. This is too many people to join in a single action.

50. **Commonality and Predominance.** There are questions of law and fact common to the Class that predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

a. Whether UW Medicine failed to adequately safeguard Plaintiffs and the Class' patient information and/or PHI?

b. Whether UW Medicine failed to take reasonable steps to protect Plaintiff's and Class' patient information and/or PHI;

c. Whether UW Medicine violated the HIPAA Security rules and regulations;

d. Whether UW Medicine breached implied or express contracts to Plaintiffs and the Class;

e. Whether UW Medicine breached a common law duty of care it owed to Plaintiffs and the Class;

CORR CRONIN LLP
1001 Fourth Avenue, Suite 3900
Seattle, Washington 98154-1051
Tel (206) 625-8600
Fax (206) 625-0900

f. Whether UW Medicine was negligent and whether such negligence harmed Plaintiffs and the Class;

g. Whether UW Medicine violated Chapter 70.02 RCW and/or state regulations;

h. Whether UW Medicine failed to reasonably and promptly disclose the Breach to Plaintiffs and the Class;

i. Whether Plaintiffs and the Class may obtain equitable and injunctive relief against UW Medicine to improve its information security practices so that UW Medicine can prevent, detect, contain, and correct data security violations in the future;

j. What security practices and policies UW Medicine should have implemented and should be required to implement as part of any injunctive relief ordered by the Court;

k. Whether UW Medicine violated Chapter 42.48 RCW and/or Washington law in connection with any of the actions referenced herein;

l. Whether UW Medicine violated Chapter 70.24 RCW and/or Washington law in connection with any of the actions referenced herein;

m. Whether UW Medicine breached its contracts with Plaintiffs and the Class; and

n. The nature and scope of the relief, including monetary and injunctive relief, to which Plaintiffs and the Class are entitled.

51. **Typicality.** Plaintiffs' claims are typical of the Class because Plaintiffs' healthcare data and/or PHI, like every other Class members' information, was misused, exposed, and/or disclosed by UW Medicine.

52. **Adequate Representation.** Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class and has retained experienced counsel that will vigorously prosecute this action on behalf of the Class.

53. **Superiority of Class Action.** A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all Class members is impracticable. Moreover, the adjudication of this controversy through a class action

CORR CRONIN LLP
1001 Fourth Avenue, Suite 3900
Seattle, Washington 98154-1051
Tel (206) 625-8600
Fax (206) 625-0900

will avoid the possibility of inconsistent and potentially conflicting adjudication of claims. There will be no difficulty in the management of this action as a class action.

54. Damages for any individual class member are likely insufficient to justify the cost of individual litigation, such that in the absence of class treatment, UW Medicine's violations of law inflicting substantial damages in the aggregate would go un-remedied.

VI. CLAIMS FOR RELIEF

FIRST CLAIM FOR RELIEF
Negligence
(On Behalf of Plaintiffs and the Class)

55. Plaintiffs incorporate all preceding allegations as if set forth in full herein.

56. UW Medicine admitted and assumed duties to Plaintiffs and the Class to implement reasonable security measures through its statements, conduct, contracts, policies, and/or procedures regarding the privacy, confidentiality, and security of healthcare data, including that it would exercise care to safeguard the Plaintiffs and the Class' PHI. Through its statements, conduct, contracts, policies, and/or procedures, UW Medicine specifically assumed the duty to comply with industry standards, including without limitation HIPAA, WAC 246-320-166, Chapter 70.02 RCW, in protecting patient information.

57. Further, by collecting, storing, and using Plaintiffs and the Class members' personal and health information, UW Medicine assumed a duty of care to Plaintiffs and the Class to secure and safeguard such information, to prevent disclosure, exposure, and/or unauthorized access to such information. UW Medicine also owed a duty of care to adopt and implement appropriate safeguards based on industry standards, applicable laws, regulations, or rules to protect Plaintiffs and the Class members' healthcare data and PHI.

58. Defendant also owed duties as a result of the physician-patient relationship that existed between UW Medicine and Plaintiffs and the Class.

59. UW Medicine breached its common law, statutory, and other duties by failing to

CORR CRONIN LLP
1001 Fourth Avenue, Suite 3900
Seattle, Washington 98154-1051
Tel (206) 625-8600
Fax (206) 625-0900

use reasonable measures to safeguard Plaintiffs and the Class' PHI and other healthcare data, and by failing to provide timely and adequate notice of the Breach.

60. The facts presently known indicate that UW Medicine was reckless or, at the very least, negligent in using, storing, managing, creating, transmitting, and/or protecting Plaintiffs and the Class' personal information. UW Medicine's conduct departed from all reasonable standards of care, including without limitation by (i) failing to adequately protect Plaintiffs and the Class' PHI and other sensitive healthcare data; (ii) failing to conduct regular security audits that could have detected risk factors that, if promptly addressed, could have prevented the Breach; (iii) failing to provide adequate and appropriate supervision of persons having access to Plaintiffs and the Class' information; (iv) failing to adopt and implement sufficient server and configuration protocols to prevent the confidential health information of 974,000 individuals from being published on the internet; (v) failing to adopt and implement appropriate storage protocols to protect Plaintiffs and the Class' confidential information; (vi) failing to adopt and implement appropriate maintenance, transfer, or transmission protocols to protect Plaintiffs and the Class' confidential information; (vii) violating HIPAA security rules and regulations; (viii) violating Chapter 70.02 RCW; (ix) failing to adopt other basic security measures to prevent the Breach; and (x) failing to provide Plaintiffs and the Class complete and timely notice of the Breach and that their PHI had been exposed and/or compromised. The full nature of UW Medicine's negligence can only be identified after a thorough investigation into the facts and events surrounding the Breach.

61. As a direct and proximate result of UW Medicine's negligent acts and omissions, Plaintiffs and the Class have suffered personal, financial, social, and compensable injuries and damages in an amount to be proven at trial. On information and belief, these include without limitation heightened risk of identity theft or healthcare fraud, crimes, and abuse, actual identity theft or healthcare fraud, crimes, and abuse, loss of privacy, the illegal sale of PHI on the black

CORR CRONIN LLP
1001 Fourth Avenue, Suite 3900
Seattle, Washington 98154-1051
Tel (206) 625-8600
Fax (206) 625-0900

market or dark web, loss of time spent addressing the Breach, including without limitation reviewing data breach letters, online healthcare accounts, invoices, statements, and credit reports, the cost of credit monitoring and identity theft insurance, reasonably foreseeable emotional distress and/or disruption of their lives and fear of future identity theft or healthcare fraud, the reasonable value of decreased credit scores and ratings, diminished value of UW Medicine's services and other breach of contract damages, lost work time, and other forms of economic and non-economic harm caused by the Breach.

62. Plaintiffs and the Class seek an order declaring that Defendant was negligent under Washington law and awarding damages in an amount to be determined at trial.

SECOND CLAIM FOR RELIEF
Violation of Chapter 70.02 RCW
(On Behalf of Plaintiffs and the Class)

63. Plaintiffs incorporate all preceding allegations as if set forth in full herein.

64. Chapter 70.02 RCW requires Defendant to implement adequate safeguards in maintaining and storing Plaintiffs and the Class' "health care information."

65. Specifically, RCW 70.02.150 requires Defendant to adopt, implement, and maintain adequate "safeguards for the security of all health care information it maintains."

66. RCW 70.02.010 defines "health care information" as "any information, whether oral or recorded in any form or medium, that identifies or can be readily associated with the identity of a patient and directly relates to the patient's health care," including "any required accounting of disclosures of health care information."

67. The database entries disclosed by UW Medicine contain health care information, in that they include descriptions of PHI "directly related" to the health care of individual patients: that is, descriptions linking named patients to specific types of treatments (e.g. "cardiology" or "ICU flow," establishing that the specific patient sought treatment for heart problems or necessitated intensive care) or to specific diagnostic tests (e.g. HIV tests).

CORR CRONIN LLP
1001 Fourth Avenue, Suite 3900
Seattle, Washington 98154-1051
Tel (206) 625-8600
Fax (206) 625-0900

Furthermore, the database itself falls within the statute's reference to a "required accounting of disclosures of health care information," since the database is exactly that: a required accounting of instances in which UW Medicine disclosed health care information to third parties. Plaintiffs expect that the full database, which has not yet been produced by UW Medicine in discovery, will contain significantly more examples of exposed health care information.

68. Plaintiffs and the Class are entitled to an order(s) under RCW 70.02 requiring Defendant to (i) engage third-party auditors to evaluate its information security management practices on a routine and periodic basis, and requiring it to correct any problems or vulnerabilities detected, (ii) adopt and successfully implement sufficient process, protocols, and procedures to prevent, detect, contain, and correct data security violations, (iii) audit, test, and train its security personnel regarding appropriate processes and procedures, (iv) institute industry standard policies to securely purge, delete, and destroy data that is no longer necessary for its services or that it is not required to store or maintain under applicable law, (v) carry out regular database scanning and security checks, (vi) routinely conduct internal training and education of personnel who work with and have access to sensitive data; (vii) adopt sufficient safeguards for the maintenance of healthcare information including measures and training to detect, mitigate, and correct misconfiguration of databases; and (viii) fully educate Plaintiffs and the Class about the threats they face and steps they can take to protect themselves in the future.

69. Pursuant to RCW 70.02.170, Plaintiffs and the Class seek attorneys' fees and litigation expenses on the basis of Defendant's violation of Chapter 70.02 RCW. Plaintiffs and the Class have complied with this Chapter.

THIRD CLAIM FOR RELIEF
Violation of Chapter 70.24 RCW
(On Behalf of Plaintiff S.A. and the Class)

70. Plaintiffs incorporate all preceding allegations as set forth in full herein.

CORR CRONIN LLP
1001 Fourth Avenue, Suite 3900
Seattle, Washington 98154-1051
Tel (206) 625-8600
Fax (206) 625-0900

71. Chapter 70.24 RCW requires healthcare providers such as Defendant to maintain strict confidentiality of patient information related to testing for sexually-transmitted diseases, including HIV, and to implement adequate policies and procedures to accomplish this goal.

72. In adopting chapter 70.24 RCW (also referred to as Washington's Omnibus AIDS Act) into law, the Legislature correctly found "that sexually transmitted diseases, by their nature, involve sensitive issues of privacy, and it is the intent of the legislature that all programs designed to deal with these diseases afford patients privacy, confidentiality, and dignity."

73. UW Medicine recklessly and/or negligently violated chapter 70.24 RCW and the rules applicable thereto by exposing the protected information of both Plaintiff S.A. and all other similarly situated class members and failing to implement and maintain adequate policies and procedures to protect such information.

74. Under RCW 70.24.084(1), "Any person aggrieved by a violation of this chapter shall have a right of action" and may recover $1,000 for each negligent violation, $10,000 for each reckless or intentional violation, attorneys' fees and costs, and "[s]uch other relief, including an injunction, as the court may deem appropriate."

75. UW Medicine is liable to Plaintiff S.A., and a class of all other similarly situated individuals, for violating chapter 70.24 RCW and the rules applicable thereto as a result of the Breach.

76. UW Medicine is liable to Plaintiff S.A., and a class of all other similarly situated individuals, for $1,000 per class member for each negligent violation, and $10,000 per class member for each reckless or intentional violation, to be determined at trial.

77. UW Medicine is liable to Plaintiff S.A., and a class of all other similarly situated individuals, for attorneys' fees and costs and such other relief, including an injunction applicable to the class as a whole, to be determined at trial.

CORR CRONIN LLP
1001 Fourth Avenue, Suite 3900
Seattle, Washington 98154-1051
Tel (206) 625-8600
Fax (206) 625-0900

FOURTH CLAIM FOR RELIEF
Violation of Washington Data Breach Disclosure Law
(On Behalf of Plaintiffs and the Class)

78. Plaintiffs incorporate all preceding allegations as if set forth in full herein.

79. Under Chapter 19.255 RCW and Chapter 42.56 RCW, UW Medicine was required to disclose the Breach "immediately following discovery" and "in the most expedient time possible and without unreasonable delay."

80. UW Medicine breached its statutory duties to notify Plaintiffs and the Class by waiting an unreasonable amount of time after learning of the Breach to notify Plaintiff and Class Members and then by failing to provide Plaintiff and Class Members complete information regarding the information that was compromised.

81. UW Medicine's failure to provide notice immediately after discovering the Breach, and provide Plaintiffs and the Class with all information they need to protect themselves, violated Chapter 19.255 RCW and Chapter 42.56 RCW. Plaintiffs and the Class have been damaged in an amount to be proven at trial.

FIFTH CLAIM FOR RELIEF
Violation of Chapter 42.48 RCW
(On Behalf of Plaintiffs and the Class)

82. Plaintiffs incorporate all preceding allegations as if set forth in full herein.

83. Chapter 42.48 RCW provides that a state agency may only disclose an "individually identifiable personal record" for research purposes if it obtains the informed written consent of the person to whom the record pertains, or, in the absence of informed written consent, only in certain other statutorily-defined instances.

84. Chapter 42.48 RCW defines "individually identifiable" as any record containing "information which reveals or can likely be associated with the identity of the person or persons to whom the record pertains." It defines "personal record" as "any information obtained or maintained by a state agency which refers to a person and which is declared exempt from public

CORR CRONIN LLP
1001 Fourth Avenue, Suite 3900
Seattle, Washington 98154-1051
Tel (206) 625-8600
Fax (206) 625-0900

disclosure, confidential, or privileged under state or federal law."

85. The database entries exposed by UW Medicine constitute "individually identifiable personal records." They reveal the identities of the persons to whom the records pertain because they list individual patient names and medical record numbers. They also contain information declared exempt from public disclosure by law.

86. The information described in the database was undisputedly disclosed to researchers for the explicit purpose of research studies; the database was maintained to track such disclosures, along with other third-party disclosures of PHI, and contained descriptions of the specific PHI disclosed to the researchers and other third parties (descriptions which themselves constitute PHI). The disclosure of the database also exposed to the internet and the general public the fact that named individuals participated in specific research studies, or were considered as potential subjects for such studies based on their confidential medical records.

87. Chapter 42.48 RCW makes clear that in addition to governing the initial disclosure of the personal record by a state agency to researchers—the instances tracked in the database—the statute also requires that the state agency and the research professional enter into a legally binding agreement, extending post-disclosure, to ensure "specific safeguards to assure the continued confidentiality and security of individually identifiable records or record information" and to "prohibit any subsequent disclosure of the records or record information in individually identifiable form." In other words, both parties must continue to safeguard the confidentiality of not only the original records disclosed to researchers, but of any individually identifiable "record information," such as the descriptions of PHI found in the database.

88. By failing to secure the continued confidentiality and security of the record information in its database, leading to disclosure of the record information in individually identifiable form, UW Medicine breached Chapter 42.48 RCW.

89. State agencies and research professionals that violate any provision of Chapter

CORR CRONIN LLP
1001 Fourth Avenue, Suite 3900
Seattle, Washington 98154-1051
Tel (206) 625-8600
Fax (206) 625-0900

42.48 RCW are liable for civil penalties of $10,000 per violation.

90. The Research Act's legislative history makes unmistakably clear that the purpose of the Act was to assure that personally identifiable information about human research subjects is maintained under adequate safeguards for the protection of their privacy and other interests. The legislative history further provides that the penalty provision was provided "for unauthorized disclosure of an individual identifiable personal record or record information[.]" Thus, the language, purpose, and legislative history of the Research Acts supports both express and implied causes of action under the Research Act and Plaintiffs assert the same.

91. UW Medicine compromised the individually identifiable personal record information of approximately 974,000 individuals without their knowledge or consent in violation of Chapter 42.48 RCW. UW Medicine is therefore liable to Plaintiff and the Class members under RCW 42.48.040 for $10,000 per class member.

SIXTH CLAIM FOR RELIEF
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Class)

92. Plaintiffs incorporate all preceding allegations as if set forth in full herein.

93. UW Medicine owed and assumed in relation to Plaintiffs and the Class fiduciary duties requiring a heightened duty of care in connection with UW Medicine's component entities' physician-patient relationship to Plaintiffs and the Class.

94. The duties UW Medicine owed and assumed also included the duty of confidence.

95. UW Medicine breached these duties to Plaintiffs and the Class by, among other things, failing to exercise the utmost duty of care in protecting their personal healthcare information from unauthorized disclosure, use, access, and/or exposure. UW Medicine also breached its fiduciary duties by failing to adopt, implement, and maintain appropriate security practices to ensure Plaintiffs and the Class' personal information was protected, and failing to

CORR CRONIN LLP
1001 Fourth Avenue, Suite 3900
Seattle, Washington 98154-1051
Tel (206) 625-8600
Fax (206) 625-0900

disclose these failures.

96. Plaintiffs and the Class have been harmed and will continue to be harmed as a foreseeable result of UW Medicine's breach of duty and confidence.

97. Plaintiffs and the Class have suffered damages in an amount to be proven at trial.

SEVENTH CLAIM FOR RELIEF
Breach of Express and Implied Contract
(On Behalf of Plaintiffs and the Class)

98. Plaintiffs incorporate all preceding allegations as if set forth in full herein.

99. UW Medicine owed Plaintiffs and the Class contractual duties to protect, safeguard, and maintain the confidentiality of Plaintiffs and the Class' health information.

100. Plaintiffs and the Class entered into express **and/or** implied contracts with UW Medicine under which Plaintiffs and the Class agreed to pay UW Medicine money in exchange for, among other things, healthcare and protection of their personal information.

101. Both the provision of healthcare and the protection of Plaintiffs' health information were material components of Plaintiffs and the Class' contracts with UW Medicine.

102. UW Medicine entered into implied **and/or** express contracts with Plaintiffs and the Class to protect their personal information from exposure caused by, among other things, internal human error and/or deficient information security practices or procedures.

103. As described herein, UW Medicine breached express or implied contracts with Plaintiffs and the Class by failing to implement and maintain adequate security measures to safeguard Plaintiffs and the Class' information as promised, resulting in the exposure of Plaintiffs and the Class' personal information. As a result, Plaintiffs and the Class did not receive what they paid for, i.e. the full benefit of their bargain with UW Medicine for which they are entitled to be made whole.

104. The contracts breached include UW Medicine's promise to safeguard its patients' information, to promptly inform them of any breach, and not to disclose such

CORR CRONIN LLP
1001 Fourth Avenue, Suite 3900
Seattle, Washington 98154-1051
Tel (206) 625-8600
Fax (206) 625-0900

information to unauthorized third parties, as expressly stated in: (a) the Joint Notice of Privacy Form, which promises that UW Medicine will "let you know promptly if a breach occurs that may have compromised the privacy or security of your information" and that it will "not use or share your information other than as described here unless you tell us we can in writing," (b) the Notice of Privacy Practices Acknowledgment Form, which all patients sign to acknowledge receipt of the Joint Notice of Privacy Form and which reaffirms UW Medicine's "responsibility to protect the privacy of your information, [and] … follow the information practices that are described in this notice," (c) UW Medicine's Compliance Policy 102, posted on its website, which promises patients that it will "safeguard[] the confidentiality, integrity, and availability of PHI in all forms (including verbal, paper and electronic) and in all locations" and that its workforce members are "personally and professionally responsible for appropriately protecting PHI to which they are given access," and (d) UW Medicine's Compliance Policy 103, posted on its website, which promises that UW Medicine "takes reasonable precautions to ensure that uses of, disclosures of, or requests for PHI are limited to the minimum necessary."

105. By failing to safeguard Plaintiffs' PHI, by exposing it to Google and thereby to various third parties without Plaintiffs' express permission, and by failing to timely discover and inform patients of the disclosure, UW Medicine breached these promises.

106. It is well established that a company's privacy policies will support a breach of contract claim where "it may be inferred that the policy is 'part and parcel' of the defendant's offer of services to the plaintiff." *Gardner v. Health Net, Inc.*, No. CV 10-2140 PA (CWX), 2010 WL 11597979, at *6 (C.D. Cal. Aug. 12, 2010); *see also In re JetBlue Airways Corp. Privacy Litig.*, 379 F. Supp.2d 299, 325 (E.D.N.Y. 2005) (airline's online privacy policy gave rise to contract where plaintiffs made flight reservations in reliance on promises contained therein). Here, UW Medicine required patients to sign an acknowledgment of receipt of its privacy policies prior to receiving treatment, and Plaintiffs relied on the promises contained in

CORR CRONIN LLP
1001 Fourth Avenue, Suite 3900
Seattle, Washington 98154-1051
Tel (206) 625-8600
Fax (206) 625-0900

these policies in choosing to obtain health care from UW Medicine.

107. Moreover, although UW Medicine is required to follow federal and state law relating to PHI, its own privacy policies (as quoted above) reflect a claimed commitment to safeguard PHI that complements or goes beyond its preexisting legal duties. In *In re Anthem, Inc. Data Breach Litigation*, Case No. 15-MD-02617-LHK, 2016 WL 3029783, at *12 (N.D. Cal. May 5, 2016), the Court allowed a breach of contract claim against a health insurance company to proceed where the company's privacy policies both restated its legal obligations and also made general promises, such as promising "safeguards" to "guard confidentiality" and assuring customers they "have set up a number of policies and practices to help make sure your PII is kept secure," that "could be read to reflect a commitment by [the health insurance company] to implement privacy policies that complement (or go beyond) [the health insurance company]'s preexisting legal duties."

108. UW Medicine's privacy policies, like those in *In re Anthem*, make statements (as quoted above) reflecting a general commitment to ensure patient privacy that complements and does not merely reiterate preexisting legal duties. UW Medicine's actions in ensuring Plaintiffs acknowledged its promises prior to receiving treatment, and Plaintiffs' reliance on that promise prior to paying for healthcare and disclosing sensitive information, also establish that the parties formed an implied contract that UW Medicine would protect Plaintiffs and the Class' healthcare data.

109. In addition to breaching its privacy policies as identified above, UW Medicine breached contracts specifically entered into by Plaintiff Stacy Edwards. Ms. Edwards attended a sleep clinic at Harborview Medical Center in 2015-2017, subject to express and implied agreements. Ms. Edwards has requested her records, including these contracts, and she will amend her allegations to attach any agreements that are applicable to this case.

110. Plaintiff and the Class have been damaged by UW Medicine's breach of express

CORR CRONIN LLP
1001 Fourth Avenue, Suite 3900
Seattle, Washington 98154-1051
Tel (206) 625-8600
Fax (206) 625-0900

and implied contracts in an amount to be proven at trial.

EIGHTH CLAIM FOR RELIEF
Restitution/Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

111. Plaintiffs incorporate all preceding allegations as if set forth in full herein.

112. Plaintiffs and the Class conferred monetary benefit on UW Medicine in the form of fees paid for healthcare and associated services.

113. UW Medicine knew of and acknowledged the monetary benefit conferred upon it by Plaintiffs and the Class.

114. A portion of the monetary benefit conferred on UW Medicine by Plaintiffs and the Class was attributable to the cost of adequate data management and security services and UW Medicine's promise that it would deliver the service of maintaining the confidentiality of Plaintiffs and the Class' personal information.

115. UW Medicine failed to provide all promised services by failing to maintain the confidentiality of Plaintiffs and the Class' personal information.

116. Under principles of equity and good conscience, UW Medicine should not be permitted to retain the money belonging to Plaintiffs and the Class.

117. Plaintiffs and the Class were damaged in an amount to be proven at trial.

VII. PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of all other Class members proposed in this Complaint, respectfully request the following relief:

1. An order certifying the Class as defined herein, appointing Plaintiffs and undersigned counsel to represent the Class and providing that steps be taken to notify the Class;

2. An order expediting discovery to determine the full nature, scope, and extent of Personal Health Information that was compromised;

CORR CRONIN LLP
1001 Fourth Avenue, Suite 3900
Seattle, Washington 98154-1051
Tel (206) 625-8600
Fax (206) 625-0900

3. An order declaring that UW Medicine's actions, as described above, constitute (i) negligence; (ii) violation of Washington's Data Breach Disclosure law; (iii) violation of HIPAA; (iv) violation of Chapter 70.02 RCW; (v) violation of Chapter 70.24 RCW, (vi) violation of Chapter 42.48 RCW, (vii) breach of express and implied contract; (viii) breach of fiduciary duty; and (ix) restitution/unjust enrichment;

4. Orders granting compulsory orders and/or injunctive and other equitable relief as is necessary to protect the interest of the Class, including order(s) achieving the following: (i) prohibiting UW Medicine from engaging in the conduct described herein; (ii) requiring UW Medicine to protect all data of its patients in accordance with state, federal, and local laws and industry standards; (iii) requiring UW Medicine to engage third-party auditors to evaluate its information security management practices on a routine and periodic basis, and requiring it to correct any problems or vulnerabilities detected; (iv) requiring UW Medicine to audit, test, and train its security personnel regarding any new or modified procedures; (v) requiring UW Medicine to institute industry standards and practices regarding the purging, deletion, and destruction of data that is no longer necessary for the provision of healthcare or that it is not required to store under applicable laws; (vi) requiring UW Medicine to institute industry standards and practices regarding the use, storage, maintenance, and transmission of health information they are required to keep under applicable state and federal law; (vii) requiring UW Medicine to carry out regular database scanning and security checks; (viii) requiring UW Medicine to routinely conduct internal training and education of personnel who work with and have access to sensitive data; (ix) requiring UW Medicine to implement adequate safeguards as required under RCW 70.02.150; and (x) requiring UW Medicine to fully educate Plaintiffs and the Class about the threats they face and steps they can take to protect themselves in the future;

5. An award of monetary relief, including without limitation actual, statutory, contract, exemplary, general and punitive damages in an amount to be determined at trial;

CORR CRONIN LLP
1001 Fourth Avenue, Suite 3900
Seattle, Washington 98154-1051
Tel (206) 625-8600
Fax (206) 625-0900

6. An award of restitution to Plaintiffs and the Class in an amount to be determined at trial;

7. An award of damages and/or statutory penalties under RCW 42.48.050 in the amount of $10,000 per individual violation, per class member;

8. An award of statutory penalties under RCW 70.24 in the amount $1,000 per class member for every negligent violation, and $10,000 per class member for every reckless or intentional violation,

9. An award of litigation expenses and attorneys' fees to the maximum extent under Chapter 70.02 RCW, Chapter 70.24 RCW, and other applicable law;

10 An order creating a common fund to provide adequate monetary relief for the Class;

11. An award of pre- and post-judgment interest to the extent permissible under Washington law;

12. Leave to amend this Complaint to conform to the evidence produced at or before trial; and

13. An award of such other and further relief as equity and justice may require.

Plaintiffs request a trial by jury.

CORR CRONIN LLP
1001 Fourth Avenue, Suite 3900
Seattle, Washington 98154-1051
Tel (206) 625-8600
Fax (206) 625-0900

DATED this 21st day of October, 2019.

CORR CRONIN LLP

s/ Steven W. Fogg

Todd T. Williams, WSBA No. 45032
Steven W. Fogg, WSBA No. 23528
John T. Bender, WSBA No. 49658
Emma Grunberg, WSBA No. 54659
1001 Fourth Avenue, Suite 3900
Seattle, WA 98154-1051
Phone: 206-625-8600
Fax: 206-625-0900
sfogg@corrcronin.com
twilliams@corrcronin.com
jbender@corrcronin.com
egrunberg@corrcronin.com

Michael K. Rhodes, WSBA No. 41911
MIX SANDERS THOMPSON, PLLC
1420 Fifth Avenue, Suite 2200
Seattle, WA 98101
Phone: 206-521-5989
Fax: 888-521-5980
mrhodes@mixsanders.com

Attorneys for Plaintiffs and the Class

CERTIFICATE OF SERVICE

The undersigned certifies as follows:

1. I am employed at Corr Cronin LLP, attorneys for Plaintiffs herein.

2. On October 21, 2019, I caused a true and correct copy of the foregoing document to be served on the following via King County E-Service and Email to:

Susan D. Fahringer
Todd M. Hinnen
David B. Robbins
Matthew P. Gordon
Erin K. Earl
Tyler S. Roberts
PERKINS COIE LLP
1201 Third Avenue, Suite 4900
Seattle, WA 98101-3099
206-359-8000 – Phone
206-359-9000 – Fax
sfahringer@perkinscoie.com
thinnen@perkinscoie.com
drobbins@perkinscoie.com
mgordon@perkinscoie.com
eearl@perkinscoie.com
troberts@perkinscoie.com

Attorneys for Defendant

I declare under penalty of perjury under the laws of the state of Washington that the foregoing is true and correct.

DATED this 21st day of October, 2019.

s/ Sharon Damon
Sharon Damon

CORR CRONIN LLP
1001 Fourth Avenue, Suite 3900
Seattle, Washington 98154-1051
Tel (206) 625-8600
Fax (206) 625-0900