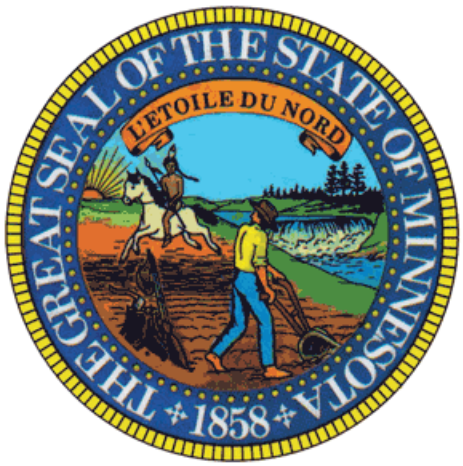
STATE OF MINNESOTA

OFFICE OF THE ATTORNEY GENERAL

Compliance Review of Fairview Health Services' Management Contracts with Accretive Health, Inc.

Volume 4
Privacy Violations



LORI SWANSON

ATTORNEY GENERAL

April 2012

Review Conducted Pursuant to Minnesota Statutes Chapters 309, 501B, and 317A

VOLUME FOUR

PRIVACY VIOLATIONS

VOLUME FOUR

PRIVACY VIOLATIONS

<u>Executive Summary</u>: Accretive Health, Inc. has violated state law by inappropriately disseminating private patient information without disclosure to or consent from patients. Accretive has violated HIPAA in the use of patient health data for purposes of collection activity. These acts have resulted in multiple violations of patient privacy rights under federal and state law.

4.1 The Right to Privacy. As long ago as the fifth century B.C., the ancient Greeks recognized the right to privacy in one of the oldest canons of western civilization, the Hippocratic Oath for doctors:

> "What I may see or hear in the course of treatment or even outside of the treatment in regard to the life of men … I will keep to myself …."

The U.S. Supreme Court has defined privacy as follows:

> "At the heart of liberty is the right to define one's own concept of existence, of meaning, of the universe…."[1]

The federal courts have extended the right to privacy to areas such as marriage,[2] procreation,[3] contraception,[4] family relationships,[5] child rearing, and education.[6] Congress further extended the right to privacy to video tape rentals,[7] cable television records,[8] drivers' license data,[9] social security numbers,[10] credit bureau information,[11] telephone records,[12] and bank financial data.[13]

The Minnesota Supreme Court has also recognized the right to privacy:

> "The right to privacy is an integral part of our humanity; one has a public persona, exposed and active, and a private persona, guarded and reserved. The heart of our liberty is choosing which parts of our lives shall become public and which parts we shall hold close."[14]

The Minnesota Legislature also passed numerous laws to recognize the right to privacy for drug abuse programs,[15] welfare data,[16] library book selections,[17] sexual assault victims,[18] pharmacist data,[19] insurance data,[20] clergy/parishioner communications,[21] and information

provided to mental health and chemical dependency therapists.[22] At the state level, the right to privacy has also been extended to attorney-client communications,[23] domestic abuse records,[24] bank data,[25] and business customer lists.[26] The privacy right in a patient's communication with her health professional is also protected by Minnesota law.[27]

4.2 The Disclosure of Medical Data Causes Real Harm. Medical information is among the most personal and private types of information about a person. Medical privacy is not only a legal, moral, and ethical obligation, but also an important part of patient treatment. Patients share the most intimate confidences with their physicians, assuming the conversations to be confidential. Health care confidentiality is designed to encourage the full and frank sharing of information between patients and their health care providers. If health records are not confidential, patients will not be candid and might forego treatment, compromising public safety, personal health, and human dignity.

A quick look at recent incidents shows why health privacy matters.

In 2001, a University of Minnesota researcher accidentally posted the names and psychological evaluations of children on the University of Minnesota's website home page.[28] In 2002, the parents of a dead child whose kidney was donated to another child were contacted by the recipient's parents, asking whether the dead child's family had any history of cancer.[29] This happened because the University of Minnesota erroneously included anonymous donor names in a mass mailing.[30] In 2009, a patient of a Fairview clinic was tested for a sexually transmitted disease because she had a new sex partner. A clinic employee copied the patient's medical records and then published a photo of the patient, her medical records, and the name of the patient's husband on a *MySpace* website entitled "Rotten Candy."[31] In 2010, six employees of the Fairmont Medical Center accessed, without authority, the medical records of a patient.[32] In

2011, approximately three dozen employees of Mercy Hospital and Unity Hospital accessed, without authority, medical records involving the hospitalization of eleven teenagers who overdosed on synthetic drugs.[33]

Medical data breaches are on the rise. The United States Department of Health and Human Services established a "Wall of Shame" in February, 2010, which now lists over 370 major incidents involving over 10 million people where medical data was breached.[34] Anecdotal examples of data breaches include an employee of the Florida Department of Health who used a list of 4,000 AIDS patients to screen potential sexual partners for himself and his friends.[35] In 2010, 20,000 emergency room patients at Stanford Hospital had their names and diagnostic information posted online for nearly a year.[36] A drug manufacturer revealed the e-mail addresses of individuals who have depression, bulimia, and obsessive compulsive disorder.[37] A congressional candidate's health records of her suicide attempt were faxed to a newspaper.[38] In 2006, a health care worker sold an FBI agent's medical records.[39] In 2007, the owner of a medical claims business submitted false Medicare claims for 1,000 patients whose records he stole.[40] In Seattle, a phlebotomist at a cancer center stole the credit card information of a cancer patient.[41] A hospital billing and collection employee used 400 stolen patient names to perpetrate a tax fraud scheme.[42] In Arkansas, a physician copied the records of a local television anchor who was raped.[43] In California, a collection agency attempting to collect from a patient disclosed the medical history of the patient and her kids to consumer credit bureaus.[44] In Arkansas, a nurse gave patient information to her husband, who attempted to blackmail the patient with it.[45] In 2003, a cardiothoracic surgeon at UCLA who thought he was about to be disciplined, retaliated by accessing the medical records of his superiors.[46] In 2011, the UCLA

Health System paid $865,000 after employees were caught examining celebrity medical records.[47]

The problem is not limited to the United States. In India, transcriptionists sell medical files to businesses. In 2009, a BBC reporter contacted two India salesmen on a website about the purchase of patient records. The salesmen said that they have under contract 17 team managers and 30,000 patient files from which they can identify the names of patients, physicians, diseases, and products desired by the patients.[48] In 2004, a Pakistani medical transcriber threatened to post patient records on the internet unless the San Francisco Medical Center settled a financial dispute.[49] In 2004, Heartland Information Services of Ohio encountered a similar extortion attempt when Bangalore workers threatened to post medical records online.[50]

Recent surveys find that patients overwhelmingly take privacy into consideration when making decisions about health treatment, with over 40% of patients withholding information due to concerns about data breaches.[51] No wonder. A patient's health data, if improperly disclosed, can affect the patient's ability to find a job, to buy insurance, to obtain credit, or even to maintain personal relationships.

As set forth below, Accretive Health, Inc.—which has entered into contracts with Fairview Health Services ("Fairview")—has handled patient data in a cavalier manner. Accretive's mishandling of patient data is not restricted to the federal Health Insurance Portability and Accountability Act of 1996 ("HIPAA").[52] The mismanagement also offends state privacy statutes.[53]

4.3 The Health Insurance Portability and Accountability Act. The HIPAA "Privacy Rule" establishes standards for the privacy of Individually Identifiable Health Information ("IIHI"), generally referred to as "Protected Health Information," or PHI. The basic

principle of the Privacy Rule is that "a covered entity" may not use or disclose protected health information, except either: (1) as the Privacy Rule permits or requires, or (2) as the individual who is the subject of the information authorizes in writing.[54] A health care provider that transmits health information in electronic form in connection with a standard transaction, such as the submission of health care claims, is a covered entity.[55]

Fairview is a "health care provider." It is comprised of hospitals and clinics that furnish health care services in the normal course of business.[56] Accretive is also a "health care provider" with respect to Fairview patients. Accretive employs nurses and social workers through its QTCC contract who provide counseling services to Fairview patients.[57]

Accretive and Fairview are "covered entities" under HIPAA because, among other things, they transmit health information in electronic form in connection with standard transactions governed by HIPAA, such as the submission of health care claims to a health plan.[58] Thus, Accretive and Fairview are required to fully comply with the HIPAA standards that govern the security, breach notification, and privacy of protected health information, as amended by the Health Information Technology for Economic and Clinical Health Act ("HITECH").[59] Accretive's own records describe the breadth of personally identifying data that qualifies certain health data as PHI:

1. Names
2. All geographic subdivisions smaller than a state
3. All elements of dates
4. Phone numbers
5. Fax numbers
6. Electronic mail addresses
7. Medical record numbers
8. Health plan beneficiary numbers
9. Account numbers
10. Certificate or license numbers
11. Vehicle identifiers and serial numbers, including license plate numbers
12. Device identifiers and serial numbers

13. Web Universal Resource Locators
14. Internet Protocol (IP) address numbers
15. Biometric identifiers, including finger or voice prints
16. Full face photographic images
17. Any other unique identifying number, characteristic or code.

(Ex. 1.)

4.4 Minnesota Privacy Laws. Minnesota Statutes section 144.293 prohibits the release of medical records without the patient's consent. It provides for a private cause of action against the provider that improperly discloses medical data. Minn. Stat. § 144.298, subd. 2.

On its website, Fairview tells its patients the following with regard to the privacy of their medical data:

> "Fairview is concerned about the privacy interests of consumers and is committed to respecting your privacy by using any personal information gathered in only the most responsible way possible. Fairview does not acquire any more information about customers than is necessary to provide efficient and secure service. **When we collect personal data, we will endeavor to disclose to you how we will use this information. Fairview will also seek to take all appropriate steps to ensure that any personal information given is protected by secure technology, including using digital signatures and other credit card data protection technology.** When Fairview collects your personal data, we may use it for research or to improve our service or website. We will ask if you want us or any of our business partners to use that information to contact you in the future about new products or services that might interest you. If you do not wish to be contacted by Fairview or any of our business partners, you can choose to have your information kept out. **Fairview gives access to personal information about consumers only to employees who require it to perform their jobs. We will take every appropriate step to keep your information secure from other employees.** If you have questions about this privacy policy, please send an e-mail to the Fairview web team."

(Ex. 2, emphasis added.)

Fairview has misrepresented to patients how their health data will be handled as it relates to the hospitals' relationship with Accretive. Minnesota law prohibits misrepresentations, false promises, and fraudulent statements to consumers.[60] Nowhere in the privacy notice does Fairview disclose that patient data will be turned over to Accretive, a third party collection

agency. Nowhere in the privacy notice does Fairview disclose that Accretive will use the data to further its efforts to collect money.

4.5 Accretive's Promises Under Its Business Associate Agreement. On February 18, 2010, Accretive and Fairview entered into a Business Associate Agreement, as required by HIPAA.[61] (Ex. 3.) Under the terms of the Agreement, Accretive agreed to administer health data as required by HIPAA and HITECH. Accretive also agreed to the following:

- It would only use patient information for the management services required under its other agreements with Fairview.
- All of the patient data shall remain the sole property of Fairview.
- Accretive will use appropriate safeguards to prevent the disclosure of the health data.
- Accretive will take appropriate steps to mitigate any effects of an unauthorized disclosure of patient information.
- Accretive will, within five days of a breach, inform Fairview of a breach.
- Accretive will make available any confidential patient data to Fairview within 10 days of a request.
- Accretive will make prompt disclosure and accounting of any disclosures of confidential patient data upon Fairview's request.
- Accretive will destroy any confidential patient information no longer required to be used in the performance of its agreement with Fairview.
- All patient information shall be kept strictly confidential.
- Accretive will maintain and use appropriate administrative, technical, and physical safeguards to ensure the confidentiality and security of the PHI it creates, receives, maintains, or transmits.
- Accretive will return all protected health information back to Fairview, or destroy such information, upon termination of the Agreement.

Fairview provided Accretive with access to virtually all patient data beginning in the spring of 2010. The data was initially maintained on the PASS system utilized by Fairview for both patient medical records and patient financial records. Thereafter, Fairview converted to the EPIC system.

4.6 "Smash and Grabs." Accretive employees operate mostly with laptops. Accretive prepared a slide presentation in February of 2011 which acknowledged that four Accretive laptops had been "smashed and grabbed" out of cars. (Ex. 4, p. 1.) In each instance,

an Accretive employee left a laptop in plain view in a locked car, the car was broken into, and the laptop was stolen. The company notes that its laptops often contain "tons of patient health and financial information." (*Id.*, p. 2.)

On June 2, 2010, an Accretive employee named Brandon Webb left an Accretive laptop in plain view in his rental car in the parking lot of an Old Mexico Restaurant in Roseville, Minnesota. A thief broke into the car and stole the laptop. (Ex. 5.) At the time, Mr. Webb was working for Accretive on the Fairview revenue cycle contract.

Accretive failed to notify Fairview that the laptop had been stolen. Fairview instead learned of the compliance breach through a series of anonymous tips and from employees who questioned the wisdom of providing confidential medical data to Accretive when it did not bother to secure the data. (Ex. 6.) In November of 2011, Fairview complained to Stephen Kelly, the Vice President of Compliance at Accretive, that Fairview was disturbed to learn that a laptop had been left in plain sight in a car and stolen. (Ex. 7.) Mr. Kelly suggested that notice was not required because the laptop was encrypted. (Ex. 8.)

About a year after Mr. Webb's laptop was stolen from his car, another Accretive employee had a "smash and grab" of his Accretive laptop from his car. On July 25, 2011, Accretive employee Matthew Doyle parked his car outside a restaurant in the Seven Corners neighborhood of Minneapolis. Once again, Mr. Doyle left the Accretive laptop in plain view of a thief, who broke into the car and stole the laptop. The laptop was not encrypted. (Ex. 9.)

The laptop contained confidential data on approximately 23,000 patients of Fairview and North Memorial Health Care, as well as data of a hospital in Detroit, Michigan. Three months after the laptop was stolen, in late October, 2011, Accretive finally responded with a report prepared by Kroll Consulting. (*Id.*) The Kroll report indicates that the laptop contained 15.4

gigabytes of data, more than 600 files containing PHI or PII, and 20 million records. The report gives no analysis as to why Mr. Doyle would comingle the patient records of various hospitals on his laptop, why he would need extensive health information about patients as a "revenue cycle" employee, why he would need to store so much patient data on his laptop, or why he would need to keep health records of Fairview patients when he was apparently now working on a revenue cycle contract with North Memorial Health Care. (*Id.*)

After the laptop theft became public, patients complained to Fairview about the invasion of privacy. At least one of the patients requested that she be provided a copy of her medical data that was on the computer. Fairview provided her with this screen shot:

First Name	Last Name	Mid. Initial	HMO ID	Patient ID	Group Number	Subscriber Number	Dependent Code	Gender	Date of Birth
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	0	[redacted]	[redacted]

Age	Months Enrolled	Active Last Day	Address 1	Address 2	City	State	Zip Code	Phone Number	Attributed TIN
[redacted]	12	Yes	[redacted]		[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Attributed Clinic	Attributed Provider	Provider (Short)	Predicted Complexity	Total Provider Allowed	Probability of IP Stay	Frail Condition	# Hospital Dominant Conditions	# Chronic Conditions	Macular Degeneration
FAIRVIEW[redacted]	[redacted]	[redacted]	2.287	$4,984.90	0.06	No	0	4	0

Bipolar Disorder	CHF	Depression	Diabetes	Glaucoma	HIV	Lipid Metabolism Disorder	Hypertension	Hypothyroidism	Immune Suppresion / Transplant
1	0		1	0	0	1	0	1	0

Ischemic Heart Disease	Osteo-porosis	Parkinsons	Asthma	Arthritis	Schizo-phrenia	Seizure Disorder	COPD	Renal Failure	Low Back Pain
0	0	0	0	0	0	1	0	0	0

Bipolar Disorder	CHF	Depression	Diabetes	Glaucoma	HIV	Lipid Metabolism Disorder	Hypertension	Hypothyroidism	Immune Suppresion / Transplant
--	--		Good	--	--	Good	--	Good	--

Ischemic Heart Disease	Osteo-porosis	Parkinsons	Asthma	Arthritis	Schizo-phrenia	Seizure Disorder	Predicted Complexity (SORTED)	Total Provider Allowed	Probability of IP Stay
--	--	--	--	--	--	--	1600	2136	1206

# Hospital Dominant Conditions	# Chronic Conditions	Top - Complexity	Top - Allowed Amt	Top - Both Complexity & Allowed Amount	Top -Either Complexity & Allowed Amount
243	366	0	0	0	0

The screen shot contains the following medical data, which is acknowledged by Accretive (Ex. 1) to be PHI under HIPAA:

- Patient's full name
- Gender

- Number of dependents
- Date of birth
- Social Security Number
- Clinic and Doctor
- A numeric score to predict the "complexity" of the patient
- A numeric score to predict the probability of an inpatient hospital stay by the patient
- The dollar amount "allowed" to the provider
- Whether the patient is in "frail condition"
- The number of "chronic conditions" the patient has
- A specific listing of certain medical conditions encountered by the patient, including:
    - Macular degeneration
    - Bipolar disorder
    - Depression
    - Diabetes
    - Glaucoma
    - HIV
    - Metabolic disorder
    - Hypertension
    - Hypothyroidism
    - Immune suppression disorder
    - Ischemic heart disease
    - Osteoporosis
    - Parkinson's disease
    - Asthma
    - Arthritis
    - Schizophrenia
    - Seizure disorder
    - Renal failure
    - Low back pain

On October 12, 2011, in response to the complaint by Fairview about employees leaving laptops in plain sight, and at about the same time Kroll was completing its report, Accretive advised its staff to hide their laptops when they leave them in their cars. (Ex. 10.)

4.7 Collection Agents Have a Straw into Fairview's Computer System. In the Kroll report, Mr. Doyle—a revenue cycle employee—acknowledged that he had been given online access to Fairview's databases. (Ex. 9, p. 7.) He wasn't the only one.

Following the Attorney General's lawsuit, the Minnesota Department of Commerce conducted an examination of Accretive's collection office in Kalamazoo, Michigan. There are approximately 100 collection agents located in the Kalamazoo facility who are in charge of both inbound and outbound telephone calls relating to the accounts receivable due from patients in hospitals under management by Accretive.

While the Minnesota Department of Commerce examination is not yet complete, the examiners have confirmed to the Attorney General's Office that collection agents had access to personal and confidential health data of Fairview patients. Some Accretive debt collectors in Kalamazoo were able to access directly the Fairview PASS system and the patient records contained in it. A screen shot from Fairview's PASS system (attached as Exhibit 11) shows the type of data available to collection agents. The first page of Exhibit 11 indicates that this patient suffered from major depression, alcohol intoxication, migraines, attention deficit disorder, and attempted suicide by cutting his wrist. The second page shows the type of treatment provided to the patient.

Accretive collection agents also have access to Fairview patient medical data through the "WinCollect" software utilized by Accretive. Attached as Exhibit 12 is a screen shot of the "WinCollect" program utilized by Accretive. The screen shot displays a box in the middle of the screen which identifies hospital information such as the patient's diagnosis, treatment, and payment history. In other words, Fairview patient data was imported by Accretive into WinCollect and then used to collect debts.

The Minnesota Department of Commerce examiners conducted interviews of several Accretive collection agents, who felt that patient medical data should not be used to collect debts. The Department of Commerce examiners also listened to recordings of telephone

conversations between Accretive's collection agents in Kalamazoo and Minnesota patients, which confirm that patient health information was used to collect debts. In addition, when Fairview's Internal Audit division asked Accretive's Kalamazoo office to supply a sample of customer calls, MFS management e-mailed a file containing PHI. (Ex. 13, p. 5.) To add insult to injury, the file was apparently e-mailed in an unsecure manner.

HIPAA, as amended by HITECH, requires that Accretive restrict its employees' access to patient protected health information. To the maximum extent possible, the employees are only supposed to have access to a "limited data set"[62] as necessary to perform their duties.[63] Only the "minimum necessary" amount of information is to be supplied to the employee for such intended purpose.[64] The privacy pledge of Fairview to patients underscores that only employees who need to know the medical information should have access to it. (*See* Section 1.4, *supra*.) Similarly, the Business Associate Agreement requires Accretive to use "appropriate safeguards" to prevent the misuse or disclosure of protected health information. (*See* Section 1.4, *supra*; *accord* 45 C.F.R. § 164.314(a)(2)(i)(A).) Accretive also agreed to keep all protected health information "strictly confidential" and to require all of its employees and subcontractors to maintain the confidentiality of protected health information. (Ex. 3.) Additionally, Accretive agreed to develop, maintain, and use all appropriate administrative, technical, and physical safeguards to preserve the confidentiality and integrity of protected health information as required by 45 C.F.R. § 164.306. (Ex. 3.)

The fact that Mr. Doyle—an Accretive revenue cycle employee—had 15.4 gigabytes of data, including protected health data on 23,000 patients of two Minnesota hospitals and data from a Michigan hospital, commingled on his laptop, underscores that Accretive does not restrict access to patient data to a "need to know" basis among its employees. Indeed, at the time his

laptop was stolen, Mr. Doyle was working on a revenue cycle contract with North Memorial, but his laptop still had protected health information about 14,000 Fairview patients. Further, Mr. Doyle supposedly was a revenue cycle employee, yet he had data apparently generated under the Quality Total Cost of Care, or QTCC, contract between Fairview and Accretive.

4.8 Unencrypted E-mails. Accretive has failed to properly encrypt e-mails containing protected health data. In December, 2011, Fairview's internal auditors described an episode in which an employee of Accretive's Medical Financial Solutions (its collection division) sent protected health information and credit card information over the Internet in an unsecure manner. (Ex. 13.) Accretive's own materials describe unencrypted e-mails as a "common Accretive HIPAA incident." (Ex. 19.)

Attached as Exhibit 14 is a transcript of apparently unencrypted e-mail discussions between several Accretive collectors concerning a patient at the University of Minnesota Medical Center. The transcript begins on the morning of June 3, 2011, with a transmission from Accretive's Samuel Johnmeyer about a patient with three upcoming visits to the hospital. He notes that she is uninsured and has an outstanding balance of $179,000. The transcript continues with the collectors discussing the condition of the patient's disease and trying to figure out if her cancer is terminal or simply disabling. The exchange ends with the collectors concerned that the uninsured patient may incur up to $40,000 in radiation bills. (*Id*.) It is troubling that Accretive's revenue cycle collectors would feel the need to discuss a patient's medical condition. It is also troubling that the e-mails do not appear to have been encrypted. The collectors are aware that the patient is uninsured and doesn't qualify for Medicaid. They need not go further in discussing her cancer.

4.9 Inadequate Encryption. It appears that when Accretive began work under the QTCC contract at Fairview, employees, on their own, had to download thirty days of "free trial offer" encryption service from the Internet if they wanted to encrypt their e-mails, because Accretive did not provide applicable encryption software. (Ex. 15.) At the end of the thirty day "free trial offer," employees simply tried to download the program again.

4.10 Password Breach in India. On January 26, 2012, at approximately the same time as the Attorney General filed the lawsuit against Accretive, a report was prepared for Accretive in which a hospital, Carondelet, part of Ascension Health, reported to Accretive that there was a password sharing incident in India. (Ex. 16.) Because of the limited information produced by Accretive, the extent to which patient information was breached is unknown. It should be noted, however, that other employees told the Attorney General's Office that Accretive employees used the log-in information of Fairview employees to download files, to which they otherwise might not have access.

4.11 Other Security Breaches. In November of 2011, Fairview and Accretive conferred about a variety of problems that Fairview had with Accretive's performance. The agenda for the meeting (Ex. 17, p. 10) states that Fairview complained that Accretive was not committed to security and that Fairview employees were able to access contract data of other hospitals under management of Accretive through their software system. (*Id.*) If the information includes pricing data with insurers, this could lead to an antitrust violation because the hospitals had access to each other's pricing information.

4.12 Transparency on Data Breaches. When confronted by Fairview about the laptop incident, Accretive is not believed to have disclosed that it had prior problems with laptop thefts. Rather, it appears that Accretive may have plotted to advise Fairview that the stolen

laptop involving Mr. Doyle was the first such incident in the company's history and that employees have access to only the "minimum necessary" data. (Ex. 18.)

In fact, Accretive's compliance officer recently prepared a PowerPoint which noted the following failures under HIPAA:

"Common Accretive HIPAA incidents:

- Laptops, unencrypted emails, too much access."

(Ex. 19.)

Conclusion. Patient privacy is one of the oldest rights known to patients and is a bedrock principle of the doctor-patient relationship. Yet, Accretive treats patient privacy in a loose and cavalier fashion. Even though patients of Fairview are assured that their health records will be protected from dissemination to third parties, Fairview has broadly shared patient data with Accretive, a licensed debt collector. Accretive has used protected patient health information to collect debts from patients; indeed, its debt collectors use the data to build credibility with patients. Accretive, whose employees' laptops contain "tons of patient health and financial information," has had multiple "smash and grabs" of laptops from cars—compromising patient privacy—and has sent unencrypted e-mails containing patient health information. Accretive has shown that it cannot be trusted to maintain the privacy of patient health information.

AG: #2991826-v1

---

[1] *Planned Parenthood v. Casey*, 505 U.S. 833, 851 (1992).
[2] *Loving v. Virginia*, 388 U.S. 1 (1967).
[3] *Skinner v. Oklahoma*, 316 U.S. 535 (1942).
[4] *Eisenstadt v. Baird*, 405 U.S. 438 (1972).
[5] *Prince v. Massachusetts*, 321 U.S. 158 (1944).
[6] *Pierce v. Society of Sisters*, 268 U.S. 510 (1925).

[7] 18 U.S.C. § 2710.
[8] 47 U.S.C. § 551.
[9] 18 U.S.C. § 2721; Minn. Stat. §§ 168.346, 171.12.
[10] 42 U.S.C. § 405 (c)(2)(C)(viii).
[11] 15 U.S.C. § 1681(a)(4).
[12] 18 U.S.C. § 2709.
[13] 12 U.S.C. § 1951.
[14] *Lake v. Walmart Stores, Inc*., 582 N.W.2d 231, 235 (Minn. 1998).
[15] Minn. Stat. § 254A.09.
[16] Minn. Stat. § 13.46.
[17] Minn. Stat. § 13.40.
[18] Minn. Stat. § 13.822.
[19] Minn. Stat. § 151.213.
[20] Minn. Stat. § 72A.502.
[21] Minn. Stat. § 595.02(1)(c); *State vs. Orfi*, 511 N.W.2d 464 (Minn. Ct. App. 1994), *review denied* (Minn. Mar. 15, 1994).
[22] Minn. Stat. § 595.02(1)(g).
[23] Minn. R. Prof. Conduct 1.6.
[24] Minn. R. Juv. Prot. P. 8.04.
[25] *Richfield Bank & Trust Co. v. Sjogren*, 309 Minn. 362, 244 N.W.2d 648 (1976).
[26] *Creative Commc'ns Consultants v. Gaylord*, 403 N.W.2d 654 (Minn. Ct. App. 1987).
[27] *See, e.g.*, Minn. Stat. Ch. 144; Minn. Stat. § 595.02, subd. 1(d), (g), and (i).
[28] Maura Lerner and Josephine Marcotty, *Web Posting has Health and University Officials Scrambling*, STAR TRIB., Nov. 8, 2001, at B1.
[29] Mike Hatch, *HIPAA: Commercial Interests Win Round Two*, 86 MINN. L. REV. 1481, 1491 (2002).
[30] Josephine Marcotty, *Names of Donors are Accidentally Included in a Letter to Kidney Patients*, STAR TRIB., Jan. 15, 2002, at A1.
[31] *Yath v. Fairview Clinics, N.P.*, 767 N.W.2d 34, 39 (Minn. Ct. App. 2009).
[32] Meg Alexander, *Hospital Fires 6 Over Privacy Breach*, FAIRMONT SENTINEL, Sept. 30, 2010, http://fairmontsentinel.com/page/content.detail/id/510004.html?nav=5003 (last visited Apr. 9, 2012).
[33] Editorial, *Allina's Harsh But Justified Firings*, STAR TRIB., May 14, 2011, at A1.
[34] Breaches affecting 500 or More Individuals, U.S. Department of Health and Human Services, www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html.
[35] Sarah Tippit, *AIDS List Leak Causes Concern Over Security of Health Records*, CHI. SUN TIMES, Oct. 14, 1996, at 22.
[36] Kevin Sack, *Patient Data Posted Online in Major Breach of Privacy*, N.Y. TIMES, Sept. 8, 2011, http://www.nytimes.com/2011/09/09/us/09breach.html?pagewanted=all.
[37] Robert O'Harrow, *Prozac Maker Reveals Patient Email Addresses*, WASH. POST, July 4, 2001, at E1.
[38] AMITAI ETZIONI, THE LIMITS OF PRIVACY 141 (1999).
[39] *United States v. Ramirez*, No. 7:05CR00709 (S.D. Tex. 2005).
[40] *United States v. Ferrer*, No. 06-60261 CR-COHN (S.D. Fla. Sept. 7, 2006).
[41] *United States v. Gibson*, No. CR04-374RSM, 2004 WL 2188280 (W.D. Wash. Aug. 19, 2004).

[42] *United States v. Williams*, No. 1:06-CR00129-UNA (D. Del. Nov. 16, 2006).
[43] *United States v. Holland*, 4:09-cr-00168-HLJ (E.D. Ark. 2009).
[44] *Brown v. Mortensen*, 253 P.3d 522 (Cal. 2011).
[45] *United States v. Smith*, 4:07-cr-00378-SWW (E.D. Ark. 2008).
[46] *United States v. Zhou*, No. 08CR01356 (C.D. Cal. 2008).
[47] *California Hospital System Pays $865,000 to Settle Medical Privacy Cases of Two Celebrities*, Pro Publica, July 7, 2011, *available at* http://www.propublica.org/article/ucla-health-system-pays-865000-to-settle-celebrity-privacy-allegations (last visited Apr. 10, 2012).
[48] Chris Rogers, *Tonight* (ITV television broadcast Oct. 18, 2009).
[49] David Lazarus, *How One Offshore Worker Sent Tremor Through Medical System*, S.F. CHRON., March 28, 2004, at A1.
[50] David Lazarus, *Extortion Threat to Patients' Records: Clients Not Informed of India Staff's Breach*, S.F. CHRON, April 2, 2004, at A1.
[51] Press Release, *Nationwide Survey Reveals Privacy Concerns Impact Healthcare Decisions Among Canadian Patients and Outcomes of Patient Care*, FairWarning, Inc., Jan. 26, 2012, *available at* http://www.marketwatch.com/story/nationwide-survey-reveals-privacy-concerns-impact-healthcare-decisions-among-canadian-patients-and-outcomes-of-patient-care-2012-01-26 (last visited Apr. 9, 2012).
[52] *See* Pub. L. 104-191, §§ 261-64 (authorizing the Secretary of Health and Human Services to issue privacy regulations governing health information); 45 C.F.R. pt. 160, 164.
[53] Minn. Stat. §§ 144.291-.298, 144.651, subd. 16.
[54] *Summary of HIPAA Privacy Rule*, U.S. Department of Health and Human Services, at 1 (May 2003) *available at* http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacy summary.pdf.
[55] 42 U.S.C. §§ 1320d-1(a)(3), 1320d-2(a); 45 C.F.R. §§ 160.102(a)(3), .103.
[56] *See* 42 U.S.C. §§ 1320d(3), 1395x(s), (u); 45 C.F.R. § 160.103.
[57] 42 U.S.C. § 1320d(3); 45 C.F.R. § 160.103.
[58] 42 U.S.C. § 1320d-2(a); 45 C.F.R. § 160.103.
[59] 42 U.S.C. § 1320d-1(a); 45 C.F.R. §§ 160.102(a), .103.
[60] *See* Minn. Stat. §§ 325D.44 (Deceptive Trade Practices Act), 325F.69 (Consumer Fraud Act).
[61] 45 C.F.R. §§ 164.308(b)(4), .502(e)(2).
[62] HIPAA defines a "limited data set" as protected health information that *excludes* the following individually indentifying information: name, address, telephone number, e-mail address, social security number, medical record number, health plan beneficiary number, account number, license number, vehicle identifiers, device identifiers, URLs, IP address, biometric identifiers, and photographs. 45 C.F.R. § 164.514(e)(2).
[63] 42 U.S.C. § 17935(b); 45 C.F.R. § 164.514(d).
[64] *See* 45 C.F.R. §§ 164.502(b), .514(d).