

United States District Court
EASTERN DISTRICT OF TEXAS
SHERMAN DIVISION

FRISCO MEDICAL CENTER, L.L.P.	§	
d/b/a BAYLOR MEDICAL CENTER	§	
AT FRISCO	§	
	§	
V.	§	CASE NO. 4:12-CV-37/4:15cv105
	§	Judge Mazzant
CYNTHIA A. BLEDSOE and	§	
MICHAEL R. BLEDSOE	§	

MEMORANDUM OPINION

Pending before the Court is Plaintiff’s Motion for Summary Judgment (Dkt. #190). Having considered the motion, and the lack of response thereto, the Court finds that the motion should be granted.

BACKGROUND

Plaintiff Frisco Medical Center, L.L.P. d/b/a Baylor Medical Center at Frisco (“Baylor Frisco”) is a hospital that provides a broad range of surgical procedures and health care for residents of North Texas. As part of its delivery of quality health care, as a health care facility, Baylor Frisco is subject to the Health Insurance Portability and Accountability Act (“HIPAA”), and must enact safeguards to ensure that protected health information pertaining to individuals or patient-identifying information that is protected from disclosure by HIPAA is not disclosed or disseminated. Baylor Frisco also has a peer review committee that conducts peer review activities, which are privileged and confidential. Baylor Frisco has developed, compiled, and maintained a substantial amount of non-public, patient health information, as well as confidential and proprietary information and trade secrets, including, without limitation, information relating to its delivery of patient care, marketing, safety practices, and strategic planning.

Baylor Frisco actively seeks to maintain the confidentiality of such information by requiring employees to agree to and execute confidentiality agreements, pursuant to which its employees agree to maintain the confidentiality of Baylor Frisco's confidential information and to refrain from disseminating such information.

Defendant Cynthia A. Bledsoe ("Ms. Bledsoe") is a registered nurse who was employed by Baylor Frisco in various capacities from 2002 to November 2011. On or about September 1, 2011, she was promoted from Sr. Vice President, Operations, to Chief Operating Officer ("COO") of Baylor Frisco. On or about August 7, 2002, Ms. Bledsoe signed a Confidentiality and Security Agreement, pursuant to which she agreed as follows:

I understand that Frisco Medical Center (the "Hospital")... must assure the confidentiality of its human resources, payroll, fiscal, research, internal reporting, strategic planning, communications, computer systems and management information (collectively, with patient identifiable health information, "Confidential Information").

In the course of my employment/assignment at the Hospital, I understand that I may come into possession of this type of Confidential Information. I will access and use this information only when it is necessary to perform my job related duties in accordance with the Hospital's Privacy and Security Policies. I further understand that I must sign and comply with this Agreement in order to obtain authorization for access to Confidential Information.

...

6. I will not make any unauthorized transmissions, inquiries, modifications or purgings of Confidential Information.

Ms. Bledsoe also signed a "Receipt and Acknowledgment of Frisco Medical Center Employee Handbook" (the "Acknowledgment of Employee Handbook"), pursuant to which Ms. Bledsoe represented that she understood she would be provided with confidential information that must not be used outside of the necessary course of business. The Employee Handbook also states, "[n]o one is permitted to remove or make copies of any Baylor Medical Center at Frisco records, reports or documents without prior management approval."

In her various positions with Baylor Frisco, including COO, Ms. Bledsoe had access to non-public, confidential and proprietary information, trade secrets, and patient health care information, subject to the limitations set forth in the Confidentiality and Security Agreement and Acknowledgment of Employee Handbook signed by Ms. Bledsoe, both of which delineated that such access was permitted only for job-related duties or in the necessary course of business and prohibited removal or copying of materials without approval. Ms. Bledsoe understood Baylor Frisco endeavored to protect its confidential information, and that as COO, she had responsibilities to ensure that Baylor Frisco met its responsibilities to safeguard the privacy of patient health information, as well as other confidential information.

Ms. Bledsoe resigned from Baylor Frisco on or about November 1, 2011. Ms. Bledsoe resigned from Baylor Frisco to accept a position with Forest Park. Ms. Bledsoe received a written employment offer from Forest Park on October 21, 2011, after receiving an oral offer on October 18, 2011. She accepted the offer on October 23, 2011. She believed that she might be asked to leave Baylor Frisco upon tendering her resignation.

Michael R. Bledsoe (“Mr. Bledsoe”) was employed by Baylor Frisco for approximately nine years, and most recently served as the Information Systems Administrator for Baylor Frisco. On or about August 26, 2002, Mr. Bledsoe signed a Confidentiality and Security Agreement which contained the same definition of “Confidential Information” as the Confidentiality and Security Agreement signed by Ms. Bledsoe.

On June 23, 2006, and on December 16, 2010, Mr. Bledsoe signed acknowledgments that he received Baylor Frisco’s Employee Handbook, pursuant to which Mr. Bledsoe agreed that he understood he would be provided with confidential information that must not be used outside of the

necessary course of business. As Information Systems Administrator, Mr. Bledsoe had administrative access to all network systems of Baylor Frisco, and therefore had the ability to access non-public, confidential and proprietary information, and trade secrets, subject to the limitations set forth in the Confidentiality and Security Agreement and Acknowledgments of Employee Handbook signed by Mr. Bledsoe, all of which delineated that such access was permitted only for job-related duties or in the necessary course of business and prohibited removal or copying of materials without approval. On or about December 13, 2011, Mr. Bledsoe tendered a letter of resignation stating that his last day of employment would be December 26, 2011.

After tendering her resignation, Ms. Bledsoe contacted Margaret Garcia, Baylor Frisco's Manager of Human Resources and, in a conversation about her departure, Ms. Bledsoe made a reference that "...she knew where too many bodies were buried." Upon learning about Ms. Bledsoe's comment, Baylor Frisco retained Hewlett-Packard ("HP") IT Security Investigations to conduct a forensic investigation of the computer equipment of Ms. Bledsoe and Mr. Bledsoe (collectively, "Bledsoe Defendants"). HP IT Security Investigations conducted its investigation and issued a report reflecting its findings and conclusions on January 6, 2012 (the "HP Report").

The HP Report provides a detailed description of the investigation, which included an examination of the desktop system assigned to and utilized by Ms. Bledsoe while she was employed with Baylor Frisco, as well as the examination of two laptop computers and an Apple iPad assigned to and utilized by Mr. Bledsoe while he was employed by Baylor Frisco. The investigation also included the examination and analysis of the network user home drives stored on Baylor Friscoservers for both Ms. Bledsoe and Mr. Bledsoe, as well as the Outlook Exchange accounts for both individuals, all of which were offloaded and provided to HP IT Security Investigations for

examination and analysis.

The investigation revealed that both Ms. Bledsoe and Mr. Bledsoe utilized “Dropbox,” a web-based file hosting service that uses “cloud” storage to enable users to store and share files with others across the Internet using file synchronization. When files are uploaded to Dropbox by a user, they automatically “sync” with another computer selected by the user, meaning that the files are transferred from one computer to another.

The investigation revealed that Ms. Bledsoe uploaded numerous folders and/or files containing statutorily protected patient health care information, privileged peer review materials, and highly confidential and proprietary information and trade secrets belonging to Baylor Frisco from her assigned Baylor Frisco computer to her Dropbox account from the period of October 25, 2011, through October 31, 2011.

A review of Ms. Bledsoe’s “Home” drive contained within the Baylor Frisco computer network revealed that the file “Pt info.pdf” was located within the folder/file structure “Dropbox\Medical Staff\Peer Review\PR Letters\PR086.” It appears that Ms. Bledsoe uploaded the file “Pt info.pdf” to Dropbox when she uploaded the folder “Dropbox\Medical Staff\Peer Review\PR Letters.” Sharon Kucyk, the HP forensic analyst who conducted the investigation, concluded that this file and other documents within the folder contained confidential patient information.

Upon review of these folders and/or files, Baylor Frisco determined that they contained protected confidential patient information, peer review materials, confidential and proprietary business information and trade secrets of Baylor Frisco. Baylor Frisco also concluded that the files named “Pt info.pdf” and “SKMBT_C35311103110390.PDF” contain protected health information, including the name of the patient, address, telephone number, and clinical information. The above

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.