

1 XAVIER BECERRA
Attorney General of California
2 NICKLAS A. AKERS
Senior Assistant Attorney General
3 DANIEL A. OLIVAS
STACEY SCHESSER
4 Supervising Deputy Attorneys General
LISA B. KIM (SBN 229369)
5 Deputy Attorney General
300 South Spring Street, Suite 1702
6 Los Angeles, CA 90013
Telephone: (213) 269-6369
7 Fax: (213) 897-4951
E-mail: Lisa.Kim@doj.ca.gov
8 *Attorneys for Plaintiff,*
The People of the State of California

ELECTRONICALLY FILED
Superior Court of California
County of Santa Barbara
Darrel E. Parker, Executive Officer
11/21/2017 10:47 AM
By: Sarah Sisto, Deputy

[EXEMPT FROM FILING FEES
PURSUANT TO GOVERNMENT
CODE SECTION 6103]

9
10 SUPERIOR COURT OF THE STATE OF CALIFORNIA
11 FOR THE COUNTY OF SANTA BARBARA
12

13 **THE PEOPLE OF THE STATE OF CALIFORNIA,**
14 **Plaintiff,**
15 **v.**
16 **COTTAGE HEALTH, GOLETA VALLEY**
17 **COTTAGE HOSPITAL, SANTA BARBARA**
18 **COTTAGE HOSPITAL, AND SANTA YNEZ**
VALLEY COTTAGE HOSPITAL,
19 **Defendants.**

Case No. 17CV05269

**COMPLAINT FOR INJUNCTION, CIVIL
PENALTIES, AND OTHER EQUITABLE
RELIEF**

(CIVIL CODE § 56.101; BUS. & PROF.
CODE, § 17200, *et seq.*)

**[VERIFIED ANSWER REQUIRED
PURSUANT TO CALIFORNIA CODE
OF CIVIL PROCEDURE SECTION 446]**

1 Plaintiff, the People of the State of California (“Plaintiff” or the “People”), by and through
2 Xavier Becerra, Attorney General of the State of California, alleges the following on information
3 and belief:

4 **INTRODUCTION**

5 1. Plaintiff brings this action against Cottage Health, Goleta Valley Cottage Hospital,
6 Santa Barbara Cottage Hospital, and Santa Ynez Valley Cottage Hospital (collectively referred to
7 as “COTTAGE” or “DEFENDANTS”) for violations of California’s Confidentiality of Medical
8 Information Act (“CMIA”) and Unfair Competition Law (“UCL”).

9 2. From 2011 through 2013, over 50,000 of COTTAGE’s patients had their
10 personally identifying information (PII) and electronic personal health information (ePHI)—
11 including medical history, diagnosis, laboratory test results, and medications—accessed and made
12 searchable online so that anyone with an internet connection could download and view patient
13 private medical data. COTTAGE had failed to adequately secure this information, resulting in
14 this data being indexed by Google and viewable in public search results.

15 3. Again in 2015, over 4,500 of COTTAGE’s patients had their PII and ePHI—
16 including medical record number, account number, name, address, Social Security Number,
17 employment information, admit and discharge dates, and other personal information—accessed
18 and made searchable online. COTTAGE had again failed to adequately secure this information,
19 resulting in more patient data being indexed by Google and viewable in public search results.

20 4. COTTAGE’s data breaches were symptoms of its system-wide data security
21 failures. COTTAGE failed to employ basic security safeguards, leaving vulnerable software
22 unpatched or out-of-date, using default or weak passwords, and lacking sufficient perimeter
23 security, among many other problems.

24 **PLAINTIFF**

25 5. Plaintiff is the People of the State of California. Plaintiff brings this action by and
26 through Xavier Becerra, Attorney General. The Attorney General is authorized by Civil Code
27 section 53.36(f)(1)(A) to bring actions to enforce the CMIA and Business and Professions Code
28 sections 17204, 17206, and 17207 to bring actions to enforce the Unfair Competition Law (UCL).

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 0
- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 0
- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8

2
3
4
5

6
7
8

9
0
1

2
3
4
5

6
7
8
9
20

21

22
23
24
25
26

27
28

13. Venue is proper in this Court pursuant to Code of Civil Procedure section 395.5 because DEFENDANTS' principal places of business are situated in the County of Santa Barbara.

DEFENDANTS' BUSINESS ACTS AND PRACTICES

14. COTTAGE is a provider of medical treatment and services licensed in the State of California who, in the regular course of business, collects personal health and medical information from its patients and stores and transmits said information in electronic form. Accordingly, COTTAGE must comply with the CMIA, the Health Information Portability and Accountability Act of 1996 (HIPAA), and the California Health and Safety Code.

15. Pursuant to the CMIA, HIPAA, and the California Health and Safety Code, COTTAGE is required to safeguard the confidentiality of medical information they create, maintain, preserve, store, abandon, destroy, or dispose.

COTTAGE'S FIRST DATA BREACH

16. COTTAGE owned and operated a File Transfer Protocol server that stored aggregated data on all of its surgical patients. On this server, COTTAGE stored records that contained the following information for its surgical patients: Name; Address; Gender; Date of Birth; Medical Record Number; Hospital Account Number; Medical Information (such as operative procedure and associated clinical information); and internal tracking codes.

17. From at least December 10, 2011 to around December 2, 2013, the medical records stored on this internet-connected FTP server were not encrypted, not protected by a password, not secured behind a firewall, and did not have file access permissions configured to prevent unauthorized access. This server also allowed access via an anonymous username, meaning the files could be accessed without a verified username and password.

18. Because anonymous access was enabled on COTTAGE's server and it lacked other basic security safeguards, the data was exfiltrated off the server hundreds of times. The medical records on the server were also accessed and indexed by Google. The records, including all of the data on its surgical patients, were available to anyone with an Internet connection and

1 presented as a returned Google search result. The files, including the PII and PHI, could be
2 accessed and viewed by clicking on a hyperlink.

3 19. On December 2, 2013, an individual in Arizona notified COTTAGE that he had
4 discovered and accessed the medical records from this server when he was doing an internet
5 search via Google.

6 20. COTTAGE determined the identity of its patients who had their PII and ePHI
7 exposed on this FTP server. COTTAGE found that over 50,000 individuals had their medical
8 information on the unprotected server.

9 21. Subsequent security assessments found that both COTTAGE's external and
10 internal information and systems were significantly compromised. COTTAGE was running
11 outdated software, failing to apply software patches, not resetting default configurations, not
12 using strong passwords, failing to limit access to sensitive PII, and failing to conduct regular risk
13 assessments, among other things.

14 COTTAGE'S SECOND DATA BREACH

15 22. On or about November 8, 2015, COTTAGE discovered that another server that it
16 owned and operated was accessible on the internet and had been indexed by search engines.

17 23. This second server was also unprotected by a firewall, even though it contained
18 sensitive personal health information of COTTAGE patients. From October 26, 2015 until
19 November 8, 2015, misconfigured server settings allowed the server to be accessed and indexed
20 by known search engines, including Google, and by a limited number of other unidentified
21 parties.

22 24. This data breach exposed the PII and/or the ePHI of another 4,596 COTTAGE
23 patients. External parties could access patients' medical record number, account number, name,
24 address, Social Security Number, employment information, admission and discharge dates, and
25 other personal information.

1 **FIRST CAUSE OF ACTION**

2 **VIOLATIONS OF THE CONFIDENTIALITY OF MEDICAL INFORMATION ACT**

3 **CIVIL CODE SECTION 56.101**

4 **(Failure to Preserve Confidentiality of Medical Information)**

5 25. The People reallege and incorporate by reference each of the paragraphs above as
6 though fully set forth herein.

7 26. COTTAGE is obligated to preserve the confidentiality of medical information it
8 creates, maintains, preserves, stores, abandons, destroys, or disposes. [Civ. Code § 56.101(a).]

9 27. COTTAGE failed to maintain, preserve, and store medical information in a
10 manner that preserves the confidentiality of the information. Among other things, COTTAGE
11 stored PII and ePHI on its servers in a manner where it could be, and was accessed by
12 unauthorized individuals.

13 28. Because of COTTAGE's failures, COTTAGE negligently maintained, preserved,
14 and stored medical information in violation of Civil Code section 56.101(a).

15 29. COTTAGE also negligently disclosed medical information in violation of Civil
16 Code section 56.36(c)(1). COTTAGE's failure to implement reasonable security safeguards on at
17 least two servers that allowed internet search engines, such as Google, to publicly index and
18 collect confidential medical information and make it available to anyone with internet access.
19 COTTAGE's actions caused confidential medical information to be released to and accessed by
20 the public.

21 **SECOND CAUSE OF ACTION**

22 **VIOLATIONS OF BUSINESS AND PROFESSIONS CODE**

23 **SECTION 17200, *ET SEQ.***

24 **(Unlawful, Unfair, and Fraudulent Business Practices)**

25 30. The People reallege and incorporate by reference each of the paragraphs above as
26 though fully set forth herein.

31. COTTAGE has engaged in unlawful, unfair, or fraudulent acts or practices, which constitute unfair competition within the meaning of Section 17200 of the Business and Professions Code.

32. Specifically, COTTAGE has violated the following laws:

(a) Civil Code section 56.101(a), which requires COTTAGE to create, maintain, preserve, and store medical information in a manner that preserves the confidentiality of the information contained therein;

(b) Health & Safety Code § 123149(g), which requires COTTAGE to develop and implement policies and procedures to include safeguards for confidentiality and unauthorized access to electronically stored patient health records, authentication by electronic signature keys, and systems maintenance; and

(c) 42 U.S.C.A. § 1320d-2(d)(2), which requires COTTAGE to maintain reasonable and appropriate administrative, technical, and physical safeguards to ensure the integrity and confidentiality of medical information and to protect against reasonably anticipated threats or hazards to the security or integrity of the information; and unauthorized uses or disclosures of the information.

33. The above-referenced laws apply to COTTAGE because it is a health care provider licensed in the State of California who creates, maintains, receives, and transmits protected health information electronically.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

1. Pursuant to Business and Professions Code section 17203, that the Court enter all orders necessary to prevent Cottage, its successors, agents, representatives, employees, and all persons who act in concert with Cottage from engaging in any act or practice that constitutes unfair competition in violation of Business and Professions Code section 17200, including as alleged in this Complaint;

2. Pursuant to Civil Code section 56.36(c)(1), that the Court assess a civil penalty of Two Thousand Five Hundred Dollars (\$2,500) for each violation of Civil Code section 56.101, as proved at trial;

3. Pursuant to Business and Professions Code section 17536, that the Court assess a civil penalty of Two Thousand Five Hundred Dollars (\$2,500) for each violation of Business and Professions Code section 17200, as proved at trial;

4. That Plaintiff recovers its cost of suit herein, including costs of investigation.

5. For such other and further relief as the Court deems just and proper.

Dated: November 21, 2017

Respectfully Submitted,

XAVIER BECERRA
Attorney General of California
NICKLAS A. AKERS
Senior Assistant Attorney General
DANIEL A. OLIVAS
STACEY SCHESSER
Supervising Deputy Attorneys General



LISA B. KIM
Deputy Attorney General
*Attorneys for Plaintiff,
The People of the State of California*

SA2014312234
52425631_4.doc