Filed 5/21/14

CERTIFIED FOR PUBLICATION

IN THE COURT OF APPEAL OF THE STATE OF CALIFORNIA

FOURTH APPELLATE DISTRICT

DIVISION TWO

EISENHOWER MEDICAL CENTER, Petitioner, v. THE SUPERIOR COURT OF RIVERSIDE COUNTY, Respondent; CARMEN MALANCHE et al., Real Parties in Interest.	E058378 (Super.Ct.No. INC1108128) OPINION

ORIGINAL PROCEEDINGS; petition for writ of mandate. Harold W. Hopp, Judge. Petition granted.

Horvitz & Levy, Lisa Perrochet, Steven S. Fleischman; Baker & Hostetler, Michael R. Matthias and Dawn Kennedy for Petitioner.

No appearance for Respondent.

Harris & Ruble, Alan Harris, Priya Mohan and Dave Zelenski for Real Parties in Interest.

Petitioner Eisenhower Medical Center (EMC) seeks writ review of an order denying its motion for summary adjudication of a cause of action under the Confidentiality of Medical Information Act (CMIA). (Civ. Code, § 56 et seq.)[1] We grant EMC's petition, concluding that a health care provider cannot be held liable under the relevant portions of the CMA for the release of an individual's personal identifying information that is not coupled with that individual's medical history, mental or physical condition, or treatment.

FACTUAL AND PROCEDURAL BACKGROUND

A computer was stolen from EMC on March 11, 2011, containing an index of over 500,000 persons to whom EMC had assigned a clerical record number dating back to the 1980's. The information included each person's name, medical record number (MRN), age, date of birth, and last four digits of the person's Social Security number (SSN). This information on the computer was password protected but not encrypted. A couple of weeks later, EMC sent out notice to these individuals informing them of the theft.

Real parties in interest (Plaintiffs) are a few of the individuals whose names were on the index. They filed the underlying action as a putative class action against EMC seeking nominal damages of $1,000 each under the CMIA. The complaint also includes

[1] Further statutory references are to the Civil Code, unless otherwise stated.

a second cause of action for violation of the Customer Records Act (CRA) (Civ.Code, § 1798.82), which requires notification to consumers when security systems are breached.

EMC moved for summary judgment or adjudication contending that the theft of the computer did not result in a disclosure of medical information of any of the listed persons. Information about an individual's medical history, condition, or treatment is saved only on EMC's servers located in the data center. The index that was on the stolen computer is a subset of information from its master patient index and can be used in case of a power outage or network failure to look up the patient's MRN so that a hard copy of the medical records can be located. The MRN is sequential and contains no coded information. Thus, EMC argues that the index did not contain medical information within the meaning of the CMIA, which requires a disclosure of "individually identifiable information" (which it concedes the index contained) with information "regarding a patient's medical history, mental or physical condition, or treatment." (§ 56.05, former subd. (g).)

EMC also pointed out that, upon inquiry, a general acute care hospital may disclose without consent the name, address, age, sex, and a general description of the reasons for treatment of a patient. (§ 56.16.)

As for the second cause of action under the CRA, EMC contended that it did not disclose "personal information," which includes a person's name and either of five data elements, including SSN and medical information. A truncated SSN does not qualify, it argued. In any case, it provided timely notice as required under the CRA.

Plaintiffs' opposition first contended that the summary judgment motion is moot because after filing it, they amended the complaint to allege two other computers were stolen in January 2011 resulting in violations of the CMIA. Plaintiffs also argued that EMC had reported the theft of the computer as a breach to federal authorities, the Department of Health and Human Services (HHS), so it must be considered a breach of the CMIA. Plaintiffs primarily argued that the mere fact that a person's name is on the index reveals that he or she was a patient and, thus, there has been a release of medical history. Finally, they assert that the information on the index could be used to hack into the database and perhaps access a patient's medical information.

The trial court denied summary judgment and adjudication. First, it noted that the motion did not address recent amendments to the complaint regarding additional incidents. Its denial was based principally on its belief that the fact that a person was a patient at the hospital is medical information within the meaning of the CMIA. Its order stated that it found EMC had not sustained its burden of proof that there were no triable issues of fact.

DISCUSSION

EMC seeks review only as to the first cause of action for breach under the CMIA arising from the March 2011 theft. It does not challenge the denial of summary adjudication as to the causes of action arising from the January thefts or under the CRA.[2]

---

[2] We reject plaintiffs' assertion that EMC's motion was rendered moot by the amendments regarding the January 2011 theft. When plaintiffs sought leave to file the

[footnote continued on next page]

EMC contends that "medical information" as defined under the CMIA is substantive information regarding a patient's medical condition or history that is combined with individually identifiable information. It notes here there was a disclosure or release of "individually identifiable information," but not medical information. We agree. We note the issue thus drawn is a narrow one and does not require this court to determine whether there is a distinction between a disclosure or release of medical information under the CMIA, whether EMC was negligent in handling its computer records, or whether unauthorized persons actually viewed plaintiffs' medical records.[3]

[footnote continued from previous page]
second amended complaint adding these allegations, their counsel agreed that EMC would not have to refile its motion since the legal issues raised were the same whether framed by the first or second amended complaint. Even in the introductory portion of their response to this petition, plaintiffs state that it is logical for this court to resolve the writ as though the allegations relating to the January and the March computer thefts are separate causes of action as the trial court said it would do at a hearing on December 18, 2012. Plaintiffs further indicate in their response that the second amended complaint could be treated as though it articulated four separate causes of action, two dealing with the January incident and two dealing with the March incident. Its response "is prepared as though the writ is directed to only the March breach." This indicates more than a forfeiture of the mootness, but an express waiver.

[3] In the recent decision from the Second District, *Regents of University of California v. Superior Court* (2013) 220 Cal.App.4th 549, a distinction was drawn between the terms "disclose" and "release." That court concluded that "release" does not require a showing of an affirmative communicative act by a health care provider. It went on to hold that under section 56.36, subdivision (b), as incorporated into section 56.101, more than an allegation of loss of possession by a health care provider is necessary to state a cause of action for negligent maintenance or storage of confidential medical information. What is required, according to *Regents*, is pleading, and ultimately proving, that the confidential nature of the plaintiff's medical information was breached as a result of the health care provider's negligence. The plaintiff in *Regents* could not maintain her cause of action because she could not allege that her medical records had, in fact, been viewed by an unauthorized person. The sole issue raised in our case is what constitutes

[footnote continued on next page]

The CMIA provides that no health care provider shall disclose or release medical information regarding a patient of the provider without first obtaining authorization. It specifically provides that an individual may recover $1,000 nominal damages against any person or entity who has negligently released his confidential medical information. The individual does not have to show that he suffered or was threatened with actual damages in order to recover the $1,000. (§ 56.36, subd. (b)(1).)

Section 56.05, former subdivision (g), defines "medical information" as "any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment. 'Individually identifiable' means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity."

In arriving at this conclusion, we apply some fundamental rules of statutory construction. The first rule is that the courts will adopt the plain meaning of the statute unless it would be repugnant to the obvious purpose of the statute. (*Lungren v.*

[footnote continued from previous page]
"medical information" so we need not reach the issues decided in *Regents*. Without expressing an opinion on the matter, we will use the term "release" for the sake of uniformity and convenience.

Deukmejian (1988) 45 Cal.3d 727,735 ["Words used in a statute or constitutional provision should be given the meaning they bear in ordinary use. [Citations.] If the language is clear and unambiguous there is no need for construction, nor is it necessary to resort to indicia of the intent of the Legislature (in the case of a statute) or of the voters (in the case of a provision adopted by the voters)."].) It is clear from the plain meaning of the statute that medical information cannot mean just any patient-related information held by a healthcare provider, but must be "individually identifiable information" and also include "a patient's medical history, mental or physical condition, or treatment." This definition does not encompass demographic or numeric information that does not reveal medical history, diagnosis, or care. As amicus Sutter Health notes, the Legislature has made distinctions between demographic information and medical information in several statutes, Penal Code sections 530.5, 530.55 and Civil Code section 1798.82.

Another rule of statutory construction is to give effect, whenever possible, to the statute as a whole, and to every word and clause thereof, leaving no part of the provision useless or deprived of meaning. (*California Assn. of Psychology Providers v. Rank* (1990) 51 Cal.3d 1, 18.) Applying these rules, the mere fact that a person may have been a patient at the hospital at some time is not sufficient. If interpreted as plaintiffs wish, then release by a health care provider of personal identification would be sufficient whether or not there was a release of substantive information regarding that person's medical condition, history, or treatment. Under that construction, the fact that an individual's name is on a list released by doctor X or clinic Y is sufficient to violate the

law because then it is assumed that the individual was a patient of the latter at some point. Such a construction does not comport with the plain and reasonable meaning of the statute and would render meaningless the clause "regarding a patient's medical history, mental or physical condition, or treatment."

Plaintiffs assert that a patient's medical history must include the fact that one has had medical treatment of sufficiently serious nature to warrant assignment of a medical record number and inclusion in EMC's permanent index of EMC patients. However, there is no showing that assignment of a medical record number signifies that a person has had medical treatment. It may simply mean that the person appeared at the hospital and some basic demographic information was taken. He or she may or may not have been examined and received treatment. Even accepting that the person was treated, this fact that he or she was a patient is not in itself medical information as defined in section 56.05, former subdivision (g), for the reasons discussed *ante*.[4] Plaintiffs also argue that a person's name on the index with an MRN indicates that a hard copy of his or her medical record was generated. Confirmation that a person's medical record exists somewhere is not medical information as defined under the CMIA.

[4] It was remarked during oral argument that in some cases the very fact that a person is or was a patient of certain health care providers, such as an AIDS clinic, is more revelatory of the nature of that person's medical condition, history, or treatment. We are not presented with, and express no opinion concerning, such a situation.

In this regard, it is noteworthy that the CMIA allows acute care hospitals to disclose certain patient information upon demand under section 56.16.[5] Thus, section 56.16 allows hospitals to reveal medical information as long as it fits with the described categories of general description of the reason for the treatment, the general nature of the injury, and the general condition of the patient, as well as nonmedical information. (*Garrett v. Young* (2003) 109 Cal.App.4th 1393, 1405.) While section 56.16 applies only when there has been a request for information, it does lend some support for the belief that the mere fact that a person is or was a patient is not accorded the same level of privacy as more specific information about his medical history.

Lastly, plaintiffs have contended that EMC's report to HHS of the theft of the desktop computer as a breach of health information is an admission that the index constitutes medical information within the meaning of section 56.05, former subdivision (g). However, the definition of "individually identifiable health information"[6] under

---

[5] Formerly, this section applied to all traditional health care providers but has now been restricted to acute care hospitals.

[6] "Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and:
(1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
(i) That identifies the individual; or
(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual." (45 C.F.R. 160.103 (2012).)

federal law differs markedly from that in the CMIA, so that it does not follow that EMC has conceded that the index contains medical information as defined in the latter statute.[7]

In sum, we conclude that under the CMIA a prohibited release by a health care provider must include more than individually identifiable information but must also include information relating to medical history, mental or physical condition, or treatment of the individual.

DISPOSITION

Let a peremptory writ of mandate issue directing the Superior Court of Riverside County to set aside its order denying summary adjudication as to the first cause of action for breach under the CMIA arising from the March 2011 theft and to issue a new order granting the motion in accordance with the views expressed herein.

---

[7] It should also be noted that the trial court sustained EMC's evidentiary objection to the evidence plaintiffs presented on this point—their attorney's declaration attaching printouts of information off the HHS website.

Petitioner is directed to prepare and have the peremptory writ of mandate issued, copies served, and the original filed with the clerk of this court, together with proof of service on all parties.

EMC is to recover its costs.

CERTIFIED FOR PUBLICATION

McKINSTER
Acting P. J.

We concur:

RICHLI
J.

KING
J.