2015 WL 11143173 (C.D.Cal.) (Expert Report and Affidavit)
United States District Court, C.D. California.

Dennis RUTHERFORD,
v.
PALO VERDE HEALTH CARE DISTRICT et al.

No. 513CV01247.
March 27, 2015.

FRCP Rule 26(a)(2)(B): Expert Witness Report of Ross A. Leo

Name of Expert: Ross A. Leo
Area of Expertise: Medical & Surgical >> Hospital
Representing: Defendant
Jurisdiction: C.D.Cal.

I, Ross A. Leo, will offer opinions on the matter of the reasonableness, in light of industry standards pursuant to **HIPAA** regulations, of health information records and related information being removed and retained by a Palo Verde Health District employee, during and after employment, for purposes claimed by Peter Klune (former employee), and on the obligations, if any, required of PVHD as a result and the potential administrative, civil and criminal consequences. The formation of such opinions and the rationale through which I derived such opinions is based on information provided to me:

a. Plaintiff's Ex Parte Press Release

b. PVHD 02/20/14 Press Release

c. PVHD Motion to return Documents

d. PVHD opposition to the Ex Parte re PVHD Press Release

e. **HIPAA** Provisions 45 CFR SS 164.502 on Disclosure

f. First Amended Complaint Klune v PVHD, Case 5:13-cv-01247-JAK-OP Doc 49

g. Klune Declarations in support of Opposition to Return Documents

h. PVHD Policy HA 01-040 on “Confidentiality”

i. Three samples of patient records (redacted)

j. PVHD NPP

The facts and data considered by me when forming such opinions were provided in the above and through discussion of various points in them with Counsel.

My qualifications are:

a. I have an undergraduate degree in Healthcare Administration. I have been employed in Information Systems since 1977 and have been an Information Security professional for over 30 years. I have worked internationally as a Systems Analyst/Engineer, and as a Security and Privacy Consultant. My past employers include IBM, St. Luke's Episcopal Hospital, the University of Texas, Computer Sciences Corporation, and Rockwell International. As a NASA contractor from 1998 to 2002, I was Director of Security Engineering and Chief Security Architect for Mission Control at the Johnson Space Center.

b. From 2002 to 2006, I was the Director of Information Systems, and Chief Information Security Officer for the Managed Care Division of the University of Texas Medical Branch in Galveston, Texas. I developed a complete **HIPAA** compliance program for UTMB/CMC, including design, delivery and implementation of the institutional training program for compliance. This project involved (a) development and delivery of initial training materials (electronic self-paced and classroom); (b) policies, procedures and forms development for **HIPAA** privacy and security program implementation; and, (c) **HIPAA** program testing and compliance verification operations.

c. I have served as a professional consultant and educator in the area of **HIPAA** compliance and security and over the past 12 years. In that regard, I have trained and certified nearly 2,100 professionals in **HIPAA** security and compliance. I have conducted **HIPAA** audits, risk assessments and consulting engagements for more than a decade for at least 100 clients.

My publications are as follows:

a. As a published author and recognized authority, my book, "The **HIPAA** Program Reference Handbook," published in January 2005, has since become a **HIPAA** industry reference standard.

b. In 2012 I provided the definitive entry on **HIPAA**/HITECH for the Encyclopedia of Information Technology, also for Auerbach.

c. In 2004-5, while at UTMB, I researched and authored white papers on:

i. Assessment of the Requirement for Informed Consent for Telemedicine in a Correctional Setting.

ii. Assessment of Conditions of Information Ownership vs. Custodianship, and the Duty of Care to Protect PHI.

d. In 2011, I wrote and published a white paper on Disaster Recovery in Healthcare settings for Global Knowledge.

e. In 2013, 1 wrote and published three white papers on certification of **HIPAA** compliance topics (Compliance Officer, Professional Certification for Privacy Officers, and Security Officer Certification) for the Supremus Group, a company for which I provide training and consulting services to clients.

Prior Testimony

I have not testified in court as an expert witness nor been formally deposed in any court case of any kind in the past 4 years.

Compensation Rate

My normal compensation rate is $150.00 per hour, plus expenses incurred.

My Opinions and Findings are as follows:

"PROTECTED HEALTH INFORMATION" is defined in 45 CFR 160.103, and includes many forms of "individually identifiable health information" such as patient names, addresses, birth dates, telephone numbers, social security numbers, medical record numbers, health plan beneficiary numbers. **HIPAA** regulations do not require *all* of the above elements be present to constitute Protected Health Information, only a sufficient number or combination of elements to identify the individual and associate that identity with a medical diagnosis or medical plan of care (past, present, future).

Based upon review of the documents the Plaintiffs produced in their case against PVHD related to PVHD patients, my knowledge of **HIPAA** and extensive experience in analyzing documents and information for Protected Health Information, it is clear that those documents contain Protected Health Information in written form. The documents identify individuals by name, address, date of birth, medical record number, identities of relatives and associates that individual with private medical information about each individual in a medical context.

In the papers filed by Plaintiffs that I reviewed, there is no specific statement or description of exactly how the Plaintiffs, or Mr. Klune specifically, came into possession of the Protected Health Information that they disclosed. Mr. Klune does state in his declaration that he had access to this information by virtue of his role as CEO of PVHD, but no detail is provided as to whether he personally accessed and copied/downloaded the information, whether he obtained the information through another PVHD employee or whether he came to possess the information some other way.

In the Declarations of Peter Klune dated February 6, 2014 and April 2, 2014, there are several points that are notable to my analysis. First, Mr. Klune declares in paragraph 2 of his 2/6/14 declaration that his employment extended from "May 2009 to January 22, 2013." He states later in paragraph 14 of his 2/6/14 declaration that his employment with PVHD ended on "January 22, 2014." For purposes of this report, I have assumed the correct termination date is January 22, 2013 and that the second date was a typographical error and editorial oversight.

In paragraph 3 of the 2/6/14 Klune declaration, Mr. Klune states that he and his colleagues identified alleged "unlawful activity" at PVHD, reported such findings to the PVHD Board of Directors, and later, with Board approval (by whom and precisely when this reporting was done is not stated), the same findings were reported to various governmental agencies. The records provided to me do not identify what specific information was disclosed to the Board as part of this reporting. It is my understanding that just a few patient-related documents Plaintiffs produced in their lawsuit against PVHD were actually given to the government. Those documents are identified as pages PLTF2704 and PLTF2705.

As CEO of PVHD, Klune would have had access to Protected Health Information on an actual "need-to-know" basis that had to be plainly justified under the circumstances. In **HIPAA**, the requirement to establish access privileges and verify the claimed need-to-know is found in 45 CFR §§ 164.308(b)(4) and 164.308(c)(4), and a document audit trail describing this process would normally be created to substantiate the access. This same section also makes clear that such authorization cannot be "self-authorized," but must follow an established institution process embodied in policy and procedure as an implementation of internal controls.

In his declaration, Mr. Klune did not provide any detail regarding why the private medical records and Protected Health Information of PVHD patients was necessary for anything he was doing in his investigation. Nor does he state why he would have had to take or to ever disclose unredacted copies of patient information. Pursuant to PVHD's Confidentiality policy, the Confidentiality Agreements and **HIPAA** policy signed by Mr. Klune (and by Mr. Rutherford and Ms. Barth), their authority, clearance, and access to Protected Health Information "need-to-know" are not unlimited and are never to be exercised in contravention of policy or regulation. In other words, there must always be a valid justification for accessing and reviewing any patient records or protected **HIPAA** information. The sections noted above, by enforcing the requirement to validate claimed "need-to-know" for specific information prior to granting access to it, reinforce the need to validate such claims and are an implementation of the **HIPAA** requirement to reasonably limit exposure or disclosure of Protected Health Information, called

"minimum necessary" as defined in 45 CFR 164.502(b), **164**.**514**(d). Irrespective of the reasons for the alleged investigation, **HIPAA** regulations require that any access to or disclosures of protected health information be the "minimum necessary." Therefore, assuming that the names, dates of birth, medical record number, etc., were not necessary to the investigation, access to **HIPAA**-protected information went beyond the "minimum necessary" and that is contrary to the law, regulation industry standards related to **HIPAA**. Therefore, while employed as CEO of PVHD, Mr. Klune's access to **HIPAA** information without following the requirement to reasonably limit exposure or disclosure of Protected Health Information to the "minimum necessary" is contrary to the industry standards and regulations governing **HIPAA**.

In paragraph 6 of his declaration, Mr. Klune states that on December 4, 2013, approximately one year after his separation from PVHD, he provided his lawyers a "USB drive" which contained documents he had from his time at PVHD related to the investigation. The body of documents on the USB drive included unredacted copies of the Protected Health Information provided to me (in a redacted form) and which I consider to be Protected Health Information as defined by **HIPAA**.

Mr. Klune's conduct in taking, possessing and disclosing Protected Health Information following his termination on January 22, 2013, based upon my knowledge of industry standards and **HIPAA** regulation, was not appropriate and was contrary to **HIPAA** law and regulation, explained as follows:

a. As a terminated employee, Mr. Klune no longer had any authorized access to PVHD patient records under both PVHD's policies and by **HIPAA** regulations (45 CFR § 164.308(a)(3)(i)), regardless of any prior right he had to access those records for permissible reasons.

b. Mr. Klune was required by PVHD policies and by regulation to return any and all records, inclusive of any protected **HIPAA** information, to PVHD not later than his final day of employment.

c. While **HIPAA** permits a "Covered Entity" or a "Business Associate" to use and disclose Protected Health Information for certain limited purposes, (45 CFR 164.506), Mr. Klune did not meet the definition of either a Covered Entity or a Business Associate when he took and disclosed this information following his termination.

d. Nothing Mr. Klune did following his termination by PVHD would qualify him to be a "whistleblower" under that **HIPAA** exception (45 CFR § 164.502(j)), because he was no longer a PVHD "workforce member" as that term is defined by the statute. Moreover, the information was not disclosed to an attorney by a "workforce member" for a purpose authorized by the statute.

e. The conduct of Klune (and the other Plaintiffs) in *possessing* Protected Health Information after their separation from PVHD; their subsequent disclosure of that information to their lawyers nearly a year after their separation from PVHD; their disclosure of this same information to PVHD, Ms. Sartin, Ms. Hudson, Mr. Burton and defense counsel as evidence in their lawsuit, was not authorized under any provision of **HIPAA**.

To the extent Plaintiffs remain in possession of any Protected Health Information, that is also contrary to **HIPAA**.

In paragraph 9 of his declaration, Mr. Klune states he retained the USB drive and its contents after he was terminated to assure himself of "a measure of self-protection in light of the illegality..." of the alleged conduct he had investigated and reported, saying that he kept this as proof of his not having participated in the conduct nor failing to report same. Mr. Klune's explanation does not justify his conduct. Klune's statement indicates he was *knowingly* in possession of information to which he was no longer legally entitled, and in violation of PVHD Policy HR 01-040 "Confidentiality" that he, as the former CEO of PVHD, was charged with enforcing to ensure regulatory compliance amongst all workforce members.

Mr. Klune's possession of Protected Health Information during his employment at PVID without following the "minimum use" standards was contrary to **HIPAA** law, regulations and industry standards. Next, Mr. Klune's possession of Protected Health Information following his termination is another example of his conduct being contrary to **HIPAA** law, regulations and industry

standards. His disclosure of this information to his attorneys is another example of his conduct being contrary to **HIPAA** law, regulations and industry standards. Plaintiffs' production and disclosure of that information as evidence in their case against PVHD is also contrary to **HIPAA** law, regulations, industry standards and PVHD's policies. Each example also constitutes a separate and independent example of conduct contrary to **HIPAA** law, regulations and industry standards as to each patient whose information was involved.

Mr. Klune's claim of "self-protection" (which he asserts in response to PVHD's motion for return of all Protected Health Information), has no support under the **HIPAA** law or regulations, including under the "whistleblower" provisions. Mr. Klune's explanation in his declarations does not fall within the "whistleblower" exception under **HIPAA**, and he was not a "workforce member" at the time any of the three separate layers of **HIPAA** breaches occurred. There is also no provision or exception under the **HIPAA** regulation scheme for "self-protection" of former "workforce members." Moreover, under the "whistleblower" exception of **HIPAA**, there is a requirement that the "workforce member" exercise the "Minimum Necessary" standard, which would have required Mr. Klune to reduce any Protected Health Information he claims was needed to the most minimal amount or specific limited content while still accomplishing his intended goal. There is no evidence or indication here that Mr. Klune ever attempted to do this, but instead, he took, used and disclosed Protected Health Information that was *entirely un-redacted and followed his termination from PVHD.*

In my opinion, the conduct of Mr. Klune (and possibly the other Plaintiffs) was improper, unreasonable and not consistent with industry standards given my experience, knowledge and understanding of industry standards related to **HIPAA** law and regulations. Mr. Klune admits he acted *knowingly* despite knowledge of the law and **HIPAA** policies of PVHD. Mr. Klune's refusal to return such documents when requested by PVHD is also unreasonable and put he and PVHD at risk of criminal and civil penalties. In my opinion, Mr. Klune has also acted unreasonably in his continued legal obligation to protect the privacy and security of the Protected Health Information (which survives his termination) by re-disclosing this information to known others (fellow plaintiffs), his lawyers, defense counsel, the individual Defendants and possibly others.

Finally, upon discovering the **HIPAA** violations, PVHD was required within 60 days (as required by 45 CFR §§ 164.400-414 cited below due to the volume of patients affected being over 500)to notify each affected patient of the disclosure of their Protected Health Information, to issue a press release to a local media outlet because more there than 500 patients were involved and to notify the Secretary of the United States Department of Health & Human Services, in accordance with the **HIPAA** Breach Notification Rule, 45 CFR §§ 164.400-414. It is my understanding that PVHD issued written notices to each affected patient, issued a press release and self- reported to the Department of Health & Human Services and the California Department of Health Services. Had PVHD not complied with these requirements or failed to comply within the mandated 60 day period, it would have been in violation of this same statute and thus be subject to citations and fines. The civil penalties portion of the **HIPAA** Privacy Rule indicates that this such action, in light of PVHD having knowledge of the reporting requirement and failing to comply with it, would most likely qualify as a Tier 3 violation, which involves the quality of "willful neglect," and would carry a monetary fine of no less than $10,000 and as high as $1.5 million (as escalated by the HITECH Act). Having reviewed the text of the breach notification letter and the attached press release, I can state that all points required by the Notification Rule to be covered were covered appropriately and completely. PVHD should also cooperate in any investigation undertaken by the state or federal government related to the **HIPAA** violations.

Based upon my experience, knowledge and understanding of **HIPAA** regulation and industry standards, I can attest that PVHD *acted properly* in treating the human-readable ("unsecured") paper-based information as Protected Health Information, and performing all required steps of the breach notification and reporting process described in the **HIPAA** Privacy Rule and in 45 CFR §§ 164.400-414 as noted above. Given this, PVHD *acted correctly* in its role as Covered Entity and *correctly discharged its duties* regarding its custodianship and control of the PHI in question.

I must also state that following this process is not discretionary, but is mandated by Federal Law and is *automatically* triggered once a Covered Entity or Business Associate becomes aware that the conditions and events meet the criteria stated in the **HIPAA** Privacy Rule. No court action or direction of any kind is required for compliance with **HIPAA** and no process exists of which

I am aware that would enable or empower a Court to prevent a covered entity from following the legislative scheme or to issue a retraction of any mandated notice or cause attenuation of any part of the mandated process. Similarly, no part of the **HIPAA** legislation (inclusive of HITECH, the Omnibus Rule and the related CFR entries) contains verbiage to this effect.

End of Document