NOTE: This disposition is nonprecedential.

United States Court of Appeals for the Federal Circuit

IN RE RONALD S. KARPF

2014-1035

Appeal from the United States Patent and Trademark Office, Patent Trial and Appeal Board in Serial No. 11/645,067.

Decided: July 25, 2014

CHRISTIAN J. HURT, Nix, Patterson & Roach, LLP, of Irving, Texas, argued for appellant. With him on the brief was DEREK T. GILLILAND.

MEREDITH H. SCHOENFELD, Associate Solicitor, United States Patent and Trademark Office, of Alexandria, Virginia, argued for appellee. With her on the brief were NATHAN K. KELLEY, Solicitor, and KRISTI L. R. SAWERT, Associate Solicitor.

Before O'MALLEY, REYNA, and HUGHES, *Circuit Judges.*

REYNA, *Circuit Judge.*

Ronald S. Karpf appeals from a final decision by the Patent Trial and Appeal Board ("Board") of the United

States Patent and Trademark Office ("PTO") rejecting all pending claims in U.S. Patent Application No. 11/645,067 ("the '067 application") as anticipated by U.S. Patent No. 5,845,255 ("Mayaud").[1] For the reasons below, we *vacate* the Board's decision and *remand* for further proceedings.

BACKGROUND

A. The '067 application

The '067 application is directed to an electronic medical records ("EMR") system that doctors may use to access patients' medical records and enter diagnoses and corresponding treatment instructions after patient visits. It also allows patients to access their records and receive the treatment instructions from their doctors electronically. To give patients access to and control over their own medical information, patients are given two passwords: (1) a patient password that each patient may use to log in to the system to access individual medical information, including diagnoses and treatment instructions; and (2) a patient PIN that each patient can share with those doctors to whom the patient wishes to grant access to his or her information and records and from whom the patient wishes to receive instructions. Medical personnel may only access the information and records of those patients for whom they have been provided a patient PIN. After a doctor enters treatment instructions for a given patient into the system, the system tracks the patient's access to the system to monitor compliance with the treatment instructions and provide reminders when necessary.

---

[1] *Ex parte Karpf*, No. 2010-9172, 2013 WL 1225722 (P.T.A.B. Mar. 18, 2013) ("Board Decision"), *aff'd on reh'g*, (P.T.A.B. Jul. 26, 2013) ("Reh'g Decision").

Two sets of claims are pending in the '067 application: method claims 9–18 and apparatus claims 23–25.[2] Independent claim 9 recites:

> 9. A method of using an electronic medical records (EMR) system, the method comprising:
>
> a) forming an EMR database comprising:
>
> a1) for at least one patient registered to use the EMR system, storing: patient identification data; patient password; and patient personal identification number (PIN);
>
> a2) for at least one medical practitioner registered to use the EMR system, storing: medical personnel identification data; and medical personnel password;
>
> a3) for at least one medical encounter between a patient and medical personnel, storing medical encounter data relating to the at least one medical encounter, wherein the medical encounter data includes information related to the at least one reason for the medical encounter, and at least one diagnosis by medical personnel corresponding to the medical encounter;
>
> b) allowing access to the EMR database through a patient program, in which an authorized patient has access only to information related to the authorized patient, wherein the authorized patient is assigned a patient PIN in the EMR database for controlling access to information in the EMR database related to the patient; and

---

[2] Original claims 1–8 and 19–22 were withdrawn in response to a restriction/election requirement.

> c) allowing access to the EMR database through a medical personnel data entry program, in which authorized medical personnel may access records related to a given patient only upon entry of input data corresponding to the patient PIN assigned to the given patient.

Claims 10–18 depend from claim 9 and add limitations generally directed to the storage or display of treatment guidelines, patient compliance information, and other patient information.

Independent claim 23 recites:

> 23. An article of manufacture comprising at least one machine-readable storage medium having stored therein indicia of a plurality of machine-executable control program steps, the control program comprising the steps of:
>
> a) storing patient data, including patient identification data, and patient password;
>
> b) storing medical encounter data relating to at least one medical encounter between a medical personnel and a patient, wherein the medical encounter data includes at least one reason for the medical encounter, and at least one diagnosis by medical personnel corresponding to the medical encounter; and
>
> c) storing medical condition data relating to at least one medical condition that may be deemed by medical personnel to relate to a patient as a result of a medical encounter, wherein medical condition data includes general information about a given medical condition.

Claims 24–25 depend from claim 23 and add limitations generally related to determining patient compliance and issuing a notification to non-compliant patients.

B. The Mayaud Prior Art Reference

Mayaud is prior art to the '067 application under 35 U.S.C. § 102(e). Mayaud discloses an electronic prescription management system that doctors can use to prescribe medications to patients, manage prescriptions, and communicate with pharmacies and patients. Mayaud, Abstract. The system can be used to access patients' prescription history and track the efficacy of particular medications to treat the conditions for which they were prescribed. *See*, *e.g.*, *id.* col. 14 ll. 10–31; col. 21 ll. 42–63.

To ensure that personal information is protected, Mayaud uses "patient record access codes" that can be generated by or provided to patients prior to a doctor's appointment. *Id.* col. 10 ll. 20–23. Patients can then decide whether to share their codes with doctors or other third parties on a need-to-know basis, thereby controlling access to their personal information and records. *Id.* col. 10 ll. 24–26. Mayaud also explains that users may access the system from multiple stations by using user-specific passwords, which may provide varying degrees of access depending on the users' authorization levels. *Id.* col. 10 ll. 12-19, ll. 37–43. Some of the stations may run "patient-directed data access control software" that includes "patient interface components." *Id.* col. 46 ll. 41–45. These stations are separate from the stations used by prescribers and may be located, for example, in administrative or reception areas of health care facilities. *Id.*

C. Proceedings Before the PTO

During prosecution, the PTO Examiner rejected claims 9–18 and 23–25 as anticipated by Mayaud. With respect to limitation b) in claim 9 (the "patient access limitation"), the Examiner pointed to a discussion in Mayaud regarding electronic identifiers (e.g., signature recognition) for remote electronic authorization of prescription fulfillment at the pharmacy. *See* Non-Final

Office Action at 7–8 (Feb. 4, 2009). The Examiner rejected claim 23 "for the same reason" as claim 9. *Id.* at 12.

In response, Mr. Karpf argued that Mayaud did not disclose: (1) a system to which a patient, and not simply a patient's doctor, has access; (2) a patient password for a patient to gain access to the system and the patient's own records, as opposed to a patient PIN for others to use; and (3) the specific information about individual medical encounters and other patient-related information recited in the claims. *See* Applicant's Response at 15–16 (Apr. 30, 2009). Mr. Karpf also argued that the portion of Mayaud cited by the Examiner as anticipating the patient access limitation merely referred to security measures used to verify the signature of a doctor who has prescribed medicine and, indeed, a pharmacy would not need to verify a patient's signature to determine whether a prescription has been authorized. *Id.* Mr. Karpf additionally noted that the Examiner provided no details as to how the limitations of claim 23 were specifically met by Mayaud. While acknowledging that some aspects of claim 9 may be broadly found in claim 23, Mr. Karpf pointed to specific limitations in claims 23–25 that he argued were not present in Mayaud. *Id.* at 16.

The Examiner maintained the anticipation rejection of claims 9–18 and 23–25 based on Mayaud. With respect to the patient access limitation, the Examiner pointed to Mayaud's disclosure of signature recognition. *See* Final Office Action at 10 (Jul. 16, 2009). The Examiner also continued to reject claim 23 "for the same reason" as claim 9. *Id.* at 15.

Mr. Karpf appealed the anticipation rejection to the Board, essentially repeating the same arguments made before the Examiner. *See* Applicant's Appeal Br. at 9–14 (Dec. 10, 2009). Mr. Karpf emphasized his argument that Mayaud fails to disclose both patient access to an EMR system and the use of a "patient password" for patients

themselves to gain access. *Id.* at 9–10. With respect to claims 23–25 in particular, Mr. Karpf argued that patient access to the system is implicitly required by the limitation directed to a "patient password." *Id.* at 12.

The Board affirmed the Examiner's anticipation rejection of claims 9–18 and 23–25. Regarding the patient access limitation, the Board did not rely on Mayaud's discussion of signature recognition, but found that the following paragraph in Mayaud discloses granting patients access to the system:

> Patient record access codes can, in selected instances, be **patient provided**, or **granted** by intelligent security control cards, having been furnished **to the patient** by a system administrator, or agent, prior to the physician encounter. Physician or other user access to a patient's record, or to sensitive details thereof, can thereby be restricted to a need-to-know basis. Access by third parties to physician related data can be similarly protected.

Board Decision at 6 (quoting Mayaud col. 10 ll. 20–27). The Board also found that Mayaud discloses password protection, including patient passwords, and storing patient history files and medical records, including diagnoses and the type of medical encounter data recited in the claims. *See id.* at 7. The Board noted that, to the extent that Mayaud did not disclose the specific type of medical encounter data and other patient-related information recited in the claims, those limitations constituted non-functional descriptive material not entitled to any weight in the patentability analysis. *Id.* at 7 n.5.

Mr. Karpf requested rehearing on the grounds that the Board misapprehended the distinction between giving a patient control over who may access data (as in Mayaud) and giving a patient access to the data (as required in the claims). Applicant's Request for Rehearing at 2

(May 13, 2013). The Board denied rehearing, reasoning that patient control necessarily requires that the patient have access to the system in order to create controls or restrictions for doctors to access patient's records. Reh'g Decision at 3–4. The Board also pointed, for the first time, to Figure 16 in Mayaud, which the Board argued showed devices having "patient-directed data access control software" to allow patients to access the system by way of the "patient record access codes." *Id.* at 4 (citing Mayaud col. 45 ll. 18–25; col. 46 ll. 32–49; col. 47 ll. 45–46). Finally, the Board rejected Mr. Karpf's argument that no due consideration was given to additional limitations in the dependent claims, reaffirming its view that much of Mr. Karpf's arguments were predicated on nonfunctional descriptive material. *Id.* at 5.

Mr. Karpf timely appealed to this court. We have jurisdiction pursuant to 28 U.S.C. § 1295(a)(4)(A).

DISCUSSION

We vacate the Board's decision that Mayaud anticipates claims 9–18 and 23–25. The Board's factual finding that Mayaud discloses an EMR system that patients can use to access their own information is unsupported by substantial evidence.[3]

Claims 9–18 require an EMR system "in which an authorized patient has access only to information related to the authorized patient[.]" According to the specification, patient access to the EMR system is to be distinguished from access by medical personnel. While medical personnel may use the system to update patient information or enter treatment instructions, patient access is required

---

[3] *See In re Gleave*, 560 F.3d 1331, 1335–36 (Fed. Cir. 2009) (the Board's determination regarding anticipation is a question of fact that we review for substantial evidence).

for the patient to be able to review treatment instructions and receive reminders to comply with the instructions.

Although Mayaud discloses giving patients the ability to control who may access their information, it stops short of granting patients actual access to that information through the prescription system. The closest disclosure in this regard is the single reference to a "patient interface" of the "patient-directed data access control software" that runs in stations located in administrative or reception areas of health care facilities. *See* Mayaud col. 46 ll. 35–45. That discussion, however, is silent regarding who uses the patient interface or whether patients can use it to view their individual information. Indeed, the one use of the "patient interface" that is described in Mayaud is allowing the reading of data access rights off a patient's data access control card, which does not require direct interaction between a patient and the system. *See id.* col. 46 ll. 46–49.

Likewise, Mayaud's disclosure of "patient record access codes" is insufficient to support the Board's finding regarding patient access to patient information. All Mayaud teaches is that patients may use the codes to restrict doctors' access to patient information by sharing the codes with doctors on a need-to-know basis. *See* Mayaud col. 10 ll. 20–27. There is no suggestion that patients may use the codes to access their own information through the system. Indeed, other portions of Mayaud explain that user access to system workstations is password-protected, and there is no mention of patients receiving passwords. *See id.* col. 10 ll. 32–43.

In sum, the Board's finding that Mayaud anticipates the patient access limitation of claims 9–18 lacks substantial evidence. We therefore need not address Mr. Karpf's argument that the Board raised a new ground of rejection in its rehearing decision by pointing to Figure 16 in Mayaud for the first time.

With respect to claims 23–25, the Examiner's rejection did not clearly specify any particular grounds for rejecting claim 23 beyond the "same reason" for rejecting claim 9. The Board also did not identify any grounds of rejection specific to claim 23. While the patient access limitation of claim 9 is not expressly recited in claim 23, Mr. Karpf argued before the Board that the "patient password" limitation of claim 23 implicitly requires patient access. The Board, however, did not address Mr. Karpf's argument and treated the grounds of rejection for claim 9 as if they applied equally to claim 23. Because the record is not clear regarding the grounds on which the Board relied to reject claim 23, we vacate the rejection of claims 23–25 and remand for the Board to consider in the first instance whether Mayaud's failure to disclose patient access is relevant to the anticipation of those claims.[4]

CONCLUSION

The Board's finding that Mayaud discloses an EMR system that patients can use to access their own information is unsupported by substantial evidence.

VACATED AND REMANDED

---

[4] *See Getcher v. Davidson*, 116 F.3d 1454, 1459 (Fed. Cir. 1997) (remanding to the Board for lack of a claim construction analysis as well as conclusory anticipation findings).