BEFORE THE
EMPLOYMENT APPEAL BOARD
Lucas State Office Building
Fourth floor
Des Moines, Iowa 50319

LAURA L HUBKA	:	
	:	**HEARING NUMBER:** 10B-UI-07048
Claimant,	:	
	:	
and	:	**EMPLOYMENT APPEAL BOARD**
	:	**DECISION**
WINNESHIEK MEDICAL CENTER	:	
Employer.		

N O T I C E

THIS DECISION BECOMES FINAL unless (1) a **request for a REHEARING** is filed with the Employment Appeal Board within **20 days** of the date of the Board's decision or, (2) a **PETITION TO DISTRICT COURT** IS FILED WITHIN **30 days** of the date of the Board's decision.

A REHEARING REQUEST shall state the specific grounds and relief sought. If the rehearing request is denied, a petition may be filed in **DISTRICT COURT** within **30 days** of the date of the denial.

SECTION: 96.5-2-A

D E C I S I O N

UNEMPLOYMENT BENEFITS ARE DENIED

The employer appealed this case to the Employment Appeal Board. The members of the Employment Appeal Board reviewed the entire record. A majority of the Appeal Board, one member dissenting, finds it cannot affirm the administrative law judge's decision. The Employment Appeal Board **REVERSES** as set forth below.

FINDINGS OF FACT:

The claimant, Laura L. Hubka, was employed by Winneshiek Medical Center from June 24, 2002 through April 1, 2010 as a full-time ultrasonographer. (Tr. 5, 55) She also covered for the front office answering phones (Tr. 11, 16, 59, 71) and also taking care of requests for test schedulings and precertifications regarding CT, MRI, nuclear medici1ne scans, mammograms, ultrasounds, general fluoro work, etc. (Tr. 28, 32) At the start of her hire, the claimant went through orientation which outlined all the employer's policies and HIPAA for which she signed a confidentiality agreement in acknowledgment of receipt on June 24, 2002. (Tr. 6, 9, 41, Exhibit 1 & 3) Employees have authorization to access patient information on a 'need to know' basis as it relates to their particular job responsibility. (Tr. 7, 9, 13, Exhibit 4) To determine whether an employee had a 'need to know' basis for accessing a patient's record, the employer considers "…the nature of…the information viewed…the nature of…the person's job title, duties…and if they don't line up…there is a potential breach…" (Tr. 44) This determination is made by a collaboration of several management personnel. (Tr. 52)

The employer uses a two-tier password access system for employees authorized to access MediTech, their health information system, as well as Ameritech. (Tr. 35) The system shuts down automatically after a few moments of nonuse, which helps to ensure limited access. (Tr. 57) Additionally, employees are reminded not to "…lock their computers on open or share [their] passwords…it's against policy." (Tr. 12, 33) Sometimes, however, the system remained locked 'on' so that relevant personnel would have quicker access to patient records. (Tr. 63, 79, 87-88) All employees are also re-educated on the employer's organizational policies during an annual 'Blitz' and given a test on the same to ensure that all employees have knowledge and follow the employer's policies. (Tr. 6-7, 10, 41) Ms. Hubka had always successfully passed the testing. (Tr. 7)

Ms. Hubka's responsibilities as an ultrasonographer and front office worker required her to regularly access patient information for "…consulting physicians, insurance companies, and the patients…" (Tr. 11, 59) Sometimes, the claimant accessed patient information for nonmedical reasons, as she was training another employee for the front desk. (Tr. 58-59, 60, 73, 77) In such cases, there would be no corresponding data to establish her 'need to know' basis for entry. In other instances, if the claimant requested a particular service and it was denied, there would no subsequent documentation of a procedure or test that could verify the legitimacy of the claimant's access to the medical records system. Also, if the claimant mistakenly accessed a patient's record, it would usually appear as 'non-need to know' entry. These accesses usually last for only a few seconds as opposed to minutes. (Tr. 92-94)

On September 23, 2009, a new HIPAA law went into effect (Hi-Tech Act) that required the employer to notify patients of violation of confidentiality. (Tr. 35, 40-41) Sometime in March of April of 2010 (Tr. 26, 38, 49, 52), Julia Katzer, Director of Radiology and also the claimant's immediate supervisor (Tr. 5), received "…multiple reports of breaches from other staff…" who saw Ms. Hubka make unauthorized access to patients' records. (Tr. 6, 8, 25-26) Ms. Katzer immediately initiated an investigation by having each of the reporting staff complete a privacy breach form that reiterated the company's policy that "…all staff are responsible to report any possible breaches to the direct supervisor, director of IT or the director of HIM…" (Tr. 6, 13, 28, 42, Exhibit 8) Ms. Katzer then went through the proper channels to obtain permission to perform an audit of Ms. Hubka's access into the medical records systems. (Tr. 7, 42, 51)

Ms. Katzer used the claimant's user name and password to gain access into the system, which allowed her to view all entries viewed by the claimant beginning September 23rd, 2009 through February 22, 2010. (Tr. 32, 35, 39, 42-43, Exhibit 10) The employer discovered that the claimant's first entry dated September 24, 2009 involved her accessing a pregnant employee's medical records (history and physical) for which she had no reason, as the claimant worked the front desk that day. (Tr. 15-16) Ms. Hubka made several entries that same day that were nonwork-related. (Tr. 17) In an entry dated October 14, 2009, the claimant did not work that day, but was on-call that evening. When she left work, she failed to logoff, which gave access to another employee to get into that particular record. This was also considered a breach of patient confidentiality according to company policy. (Tr. 18)

After completing the audit, and verifying that the claimant had no work-related reasons for numerous accesses, the employer presented the information to administration who decided termination was in order. (Tr. 14, Exhibit 10) The employer called the claimant into a meeting to discuss the matter. (Tr. 55) When questioned, the claimant's immediate response was "…I do not joyride through patients' charts…" (Tr. 56) When questioned about specific entries, she responded that "…I left my system

open…everybody

else uses each other's access. I did not close my system…" or she "…had no idea…" about the details of questionable accesses. (Tr. 12, 73, 75) The employer terminated Ms. Hubka for repeated breaches of security over several months time. (Tr. 18-19, Exhibit 11)

REASONING AND CONCLUSIONS OF LAW:

Iowa Code Section 96.5(2)(a) (2009) provides:

> *Discharge for Misconduct*. If the department finds the individual has been discharged for misconduct in connection with the individual's employment:
>
> The individual shall be disqualified for benefits until the individual has worked in and been paid wages for the insured work equal to ten times the individual's weekly benefit amount, provided the individual is otherwise eligible.

The Division of Job Service defines misconduct at 871 IAC 24.32(1)(a):

> *Misconduct* is defined as a deliberate act or omission by a worker which constitutes a material breach of the duties and obligations arising out of such worker's contract of employment. Misconduct as the term is used in the disqualification provision as being limited to conduct evincing such willful or wanton disregard of an employer's interest as is found in deliberate violation or disregard of standards of behavior which the employer has the right to expect of employees, or in the carelessness or negligence of such degree of recurrence as to manifest equal culpability, wrongful intent or evil design, or to show an intentional and substantial disregard of the employer's interests or of the employee's duties and obligations to the employer. On the other hand mere inefficiency, unsatisfactory conduct, failure in good performance as the result of inability or incapacity, inadvertencies or ordinary negligence in isolated instances, or good faith errors in judgment or discretion are not to be deemed misconduct within the meaning of the statute.

The Iowa Supreme court has accepted this definition as reflecting the intent of the legislature. Lee v. Employment Appeal Board, 616 N.W.2d 661, 665, (Iowa 2000) (quoting Reigelsberger v. Employment Appeal Board, 500 N.W.2d 64, 66 (Iowa 1993).

The employer has the burden to prove the claimant was discharged for work-connected misconduct as defined by the unemployment insurance law. Cosper v. Iowa Department of Job Service, 321 N.W.2d 6 (Iowa 1982). The propriety of a discharge is not at issue in an unemployment insurance case. An employer may be justified in discharging an employee, but the employee's conduct may not amount to misconduct precluding the payment of unemployment compensation. The law limits disqualifying misconduct to substantial and willful wrongdoing or repeated carelessness or negligence that equals willful misconduct in culpability. Lee v. Employment Appeal Board, 616 NW2d 661 (Iowa 2000).

The record establishes that Ms. Hubka had full knowledge of the HIPAA regulations (Tr. 68) as well as the employer's other confidentiality policies, which were reiterated and tested on an annual basis. (Tr. 6, 9, 41, Exhibit 1 & 3) The employer furnished multiple examples of inappropriate access based on a computer audit performed by Ms. Hubka's immediate supervisor, Julia Katzer. (Tr. 5, 6, 8, 25-26) Ms. Hubka admitted that she may have logged onto the system for a 'need to know' reason, and didn't log off, which would have allowed someone else to have access to a patient's medical records. (Tr. 62) Her failure to log off in such instances, in and of itself, represented a confidentiality violation. (Tr. 18) The claimant also alleges that Ms. Katzer gave her permission to log on and not log off between accessing so that the day would run smoother. (Tr. 63, 79, 87-88) However, it is more plausible that this directive was meant for the Windows program as a whole and not for the Meditech and Ameritech programs, which contained confidential patients' medical information. (Tr. 63, 79, 87-88) Ms. Hubka's testimony that she complained about Ms. Katzer's alleged directive that they leave the computer logged on to the medical records' systems and her concern for this alleged common practice 'biting them in the butt' is not credible (Tr. 70) in light of the employer's confidentiality policy and all the safeguards in place (two-tier log-in procedure with individual usernames and passwords) to ensure confidentiality. (Tr. 35)

Ms. Hubka's other defenses that she may have accessed some patients' records as part of training for another employee, or that she may have made mistakes in accessing the wrong patient's medical information, are unsubstantiated. (Tr. 64, 71-72, 92-93) If she had made a mistake, the audit would have reflected 'mistaken' entries as seconds-long versus several minutes as was generally the case. (Tr. 94) When questioned about which entries involved access for training purposes, the claimant was at a loss for explanation, which makes it more probably than not that the claimant had numerous no 'need to know' purposes for accessing so many accounts. (Tr. 71) Additionally, the claimant's supervisor provided credible testimony that it wasn't necessary for Ms. Hubka to access patients' medical records for the sake of training; there were other means available to train employees. (Tr. 92-93, 94)

As for the fellow employee who was pregnant, the claimant admitted accessing her medical records, but couldn't remember whether she was training or not. (Tr. 73, 75, 77) The fact that no ultrasound was done on this employee in close proximity to when the record was accessed tends to corroborate that there was no 'need to know' basis for accessing the pregnant employee's medical data, or likewise any other instances when the claimant made unauthorized accesses of patients' records. (Tr. 16-17, 93, Exhibit 10)

The employer, justifiably, discharged the claimant for breach of security/HIPAA violations for joyriding" through patient records on her work computer. The employer need not show that the information was "leaked" or disclosed in order to prove some sort of damage to the individual whose information was improperly accessed. Rather, all the employer need establish is that there was a policy in place for which the claimant had knowledge, and that the claimant knowingly violated that policy on several occasions. Continued failure to follow reasonable instructions constitutes misconduct. See Gilliam v. Atlantic Bottling Company, 453 N.W.2d 230 (Iowa App. 1990). An employee's failure to perform a specific task may not constitute misconduct if such failure is in good faith or for good cause. See Woods v. Iowa Department of Job Service, 327 N.W.2d 768, 771 (Iowa 1982). Ms. Hubka asserted no good faith reason other than 'maybe' she was 'training' for why she accessed several of the records at issue. Considering the employer is in the business of health care, the employer has a fiduciary responsibility to maintain confidentiality of all patient records as mandated by law, which the claimant was aware. Her failure to comply with the employer's confidentiality policy constituted a blatant

disregard for the employer's interests. We conclude that the employer satisfied their burden of proof.

DECISION:

The administrative law judge's decision dated August 16, 2010 is **REVERSED**. The claimant was discharged for disqualifying misconduct. Accordingly, she is denied benefits until such time she has worked in and has been paid wages for insured work equal to ten times her weekly benefit amount, provided she is otherwise eligible. See, Iowa Code section 96.5(2)"a".

_____
Monique F. Kuester

_____
Elizabeth L. Seiser

AMG/fnv

DISSENTING OPINION OF JOHN A. PENO:

I respectfully dissent from the majority decision of the Employment Appeal Board; I would affirm the decision of the administrative law judge in its entirety.

_____
John A. Peno

AMG/fnv