Cathy Moore is an ER manager at Santara Memorial Hospital, a regional healthcare facility established in the early 1980s in the Midwest. January this year, Doug Greater, the newly hired Chief Finance Office at Santara, sent out a memo to all managerial staff to request a task force on establishing a centralized document management system of patient record storage and retrieval. The initiative was intended to comply with HIPAA guidelines. Being one of the most senior managers on staff, Cathy was recommended to become the head of the task force.

Santara Memorial Hospital endured a fire in 1989 that burned down nearly one quarter of the facilities including its paper-based record room for patient charts and files. The board approved a rebuilt and expansion project in 1990 that not only gave the hospital the lost facilities but also added around 72,000 more sq. ft of operational space. Nonetheless, the recovery of damaged and destructed patient records was a long and difficult process since the majority of date on paper files were neither entered nor updated on the computerized databases. It is worth mentioning that over 50% of the clerical and nursing staff members have been working at Santara since the ‘80’s. Though loyalty is apparent, the level of resistance to changes is high. Without a doubt, Cathy knows that it is a daunting task she is facing.

In the first task force meeting called by Mr. Greater, he addressed that there had been inconsistency and information security issues with nursing staff saving changes of certain patients’ records, instead to the server directly, on local computer hard drives before printing out hard copies to be on file. It was reported that certain patients’ records had been stored on a number of local computers and causing confusions for physicians and the billing department. Making the case worse, three local desktop computers had a crashed hard drive and the laptop computer on a blood testing cart had been stolen one night. To remedy the problem, Doug proposes that everybody in the hospital with access to electronic patient records must save all the records and subsequent changes to the H: drive as default, a shared drive on an enterprise-grade server that’s usually locked away in a machine room with restricted access. There were 720 desktop and 110 laptop computers in the hospital, so it took 6 weeks for the task force to work with the IT department staff at Santara to perform the necessary changes on local computers. It was time consuming, but the job was done.

The new system worked out the way as expected. There were, of course, a number of complaints about the changes, but most employees adapted and became used to the new system eventually. However, one day in the staff cafeteria, Cathy overheard two co-workers in the finance office talking about Mr. Greater.

“Have you heard of the new ‘H: Drive’ thing? I wonder why some medical staff made such a fuss over it.”

“Well, that was probably because we in the finance area had started storing and sharing
files and accessed to the databases that way for a while. Give them some time. They will get used to it.”

“Hey, have you noticed that Mr. Greater have been bringing his office laptop home after work. I wonder if he had told the IT people.”

“I know, I know. He is the CFO. He should know what he is doing. Tell ya, one time, I brought my office laptop home over the weekend for a project, and the network administrator found it out. Boy, did he give me a hard time.”

Suddenly, the two finance department employees were aware of Cathy’s presence. They immediately stopped talking and left the staff cafeteria.

Cathy took her leadership with the task force seriously, so she asked the IT department if any employee in finance area had reported to bring a corporate laptop outside of Santara. The response was a “no.” One major concern Cathy had was that since Doug’s executive status gives him high level of access rights to the enterprise systems, whoever can gain access to his laptop may also gain access to databases of both financial information and patient records.

Mr. Greater is the boss of Cathy’s direct supervisor Greg Seeger, Director of Medical Services, and the hospital “Complain Desk” reports to Doug as well. Since Cathy is the person partially, if not totally, responsible for the solution, by dealing with consequences of the security problems Doug may generate, Cathy’s job may be at risk if she doesn't do anything. Hence, Cathy must take action to attempt to communicate with Mr. Greater to resolve the matter.

1. Who are the key actors?
2. What are the major issues in this case?
3. Is Doug violating the ethic code to put company’s mission-critical data and information at risk? Why or why not?
4. How would you approach Doug regarding the issue? In the process of dealing with the issue, how would you involve your direct supervisor who reports to Doug? In detailed explanation including means of communication you choose.
5. Would you do it differently if the problem is caused by employees at levels lower than that of Doug’s? How?
6. What would you do to amend to the original technical upgrade plan to reduce the risk of patient records being stolen?
**SOLUTION**

**Case # --: Double Jeopardy – Endpoint Computers and Enterprise Data Security**

**Prepared by:** Roger Yin, University of Wisconsin-Whitewater, Whitewater, Wisconsin

1. **State the problem concisely**

   Cathy Moore, an ER Manager, has been appointed the chair of a task force at Santara Hospital to explore document management solutions that are compliant with HIPPA mandates. There have been some computer theft and file mismanagement issues that threaten the integrity of the security measure. A solution to centrally store and manage the critical patient records and related files on a server cluster in a dedicated area seems to remedy the vulnerability. However, Doug Greater, the CFO at Santara and the boss of Cathy’s direct supervisor, is rumored to take company laptop computer with him home and off to business trips without logging the use. If it is true, the security problem open in case Doug’s laptop gets stolen or accessed by unauthorized persons could be severe. Cathy Moore must take action and is facing not only an ethical but also career-threatening dilemma.

2. **Point out key issues; how did they influence the problem(s)**

   Primarily, Cathy need to decide whether or not or how to discuss with Doug regarding the matter and to weigh the consequences of each choice.

   **Choice/Consequence 1:** Cathy does not talk to Doug at all. If she follows this route and pretends nothing had happened, Doug may continue taking the laptop out. Other employees might do the same. There may not be anything bad that happens. If bad things do happen, Doug will likely be penalized for that he did – or didn’t – do. Cathy may also free guilty for not discussing with Doug earlier.

   **Choice/Consequence 2:** Cathy talks to Doug directly about the matter. Doug may accept Cathy’s blunt advice and stop taking the company laptop out or at least faithfully log its off-site use. On the other hand, Doug may feel intimidated by Cathy’s act and try to “get back to her” when he gets a chance.

   **Choice/Consequence 3:** Cathy tries to talk to her direct supervisor and/or IT director regarding the issue first before attempts to communicate with Doug. This is a safer and more thoughtful way to deal with the matter since Cathy’s boss and the IT director may know a better way to approach Doug. The problem with the indirect method to notify Doug is that it may take more time to deliver the message and it could be too late to prevent a security breach.

3. **Determine management’s objectives in the case**

   Generally speaking, all levels of management in a company should be always aware of issues that may affect the business bottom line. It is imperative for all managers to sustain business operation both efficiently and effectively in an ethical manner. Every manager has a defined job responsibility, and ultimately he or she must go beyond such scope to help out one another even though the other managers are not at the same level in terms of report structure.

   In a healthcare organization, the management needs to not only concern the aforementioned common objectives but also maintain a high-level professionalism toward protecting patients’ privacy and health history. In compliance with HIPAA rules, managers cross levels at Santara Hospital should jointly ensure the confidentiality, integrity, and authenticity of
patient records are diligently maintained. Management at Santara will be help responsible and accountable if any patient’s private information is leaked or stolen.

4. Understand the company’s goals regarding this case

Santara Hospital, like all healthcare organizations in similar size and operational revenue, has well-defined goals to, first and foremost, server its customers (i.e., the patients and their family members) best interest. The sole indicator for the success of Santara will lies on satisfied (and healthy) customers who may return for similar services provided by Santara. In that case, the well-trained staff who are on the same page regarding protecting patients information seem to be supremely important.

In order to maintain best practices of HIPAA rules, a consensus must be reached among managers at Santara Hospital. Even though Doug is the Chief Finance Officer, it does not mean that he as an individual can be out of the agreement for managers as a whole to protect patients private information. Therefore, Cathy, or any managers at Santara, would be responsible to reiterate the consequences of theft or intrusion to Doug since he is taking the company laptop computer out of office without logging its usage.

5. Analyze the facts of the case as they contributed to the problem

Cathy, an ER manager at Santara Hospital and the chair of its HIPAA Compliance Task Force, was facing a dilemma when she discovered that the CFO, Doug, was jeopardizing critical corporate information by bringing a company laptop computer out of office without informing anyone, including the IT department staff. On the one hand, Doug was the person in charge of setting up enterprise-level security policies that must be compliant with HIPPA rules. On the other hand, apparently, Doug has set a problematic example for all other employees that he who sets the rules can get away from obeying the rules.

Since Doug may or may not realize his own questionable act, the consequences of Cathy’s reaction could vary. The fact, therefore, was that Doug indeed took his company laptop home and on the business trips. One can argue that a c-class executive has to have access to the corporate information system anytime, anywhere to resolve urgent issues. However, the key issue here is that IT department has not verify completely that Doug’s laptop has layers of encryption and authentication requirements to gain access to data and files store on the local hard drive and remote servers via Virtual Private Network connection over public networks.

6. Consider and write the advantages and disadvantages of each alternative

(a) Cathy does not talk to Doug at all:
Advantage: Since Cathy keeps silent, at least she won’t be pointed as “whistle blower” in the later time. Perhaps Doug would stop taking the laptop out of office due any given reasons, though the chance for that to happen is small.
Disadvantage: If Cathy confronts Doug, Doug may feel intimidated by Cathy’s act and try to “get back to her” when he gets a chance.

(b) Cathy talks to Doug directly about the matter:
Advantage: Doug may accept Cathy’s blunt advice and stop taking the company laptop out or at least faithfully log its off-site use.
Disadvantage: If Cathy confronts Doug, Doug may feel intimidated by Cathy’s act and try to “get back to her” when he gets a chance.
(c) Cathy tries to talk to her direct supervisor and/or IT director regarding the issue first before attempts to communicate with Doug:

**Advantage:** This is a safer and more thoughtful way to deal with the matter since Cathy’s boss and the IT director may know a better way to approach Doug.

**Disadvantage:** The problem with the indirect method to notify Doug is that it may take more time to deliver the message and it could be too late to prevent a security breach.

7. **Choose a solution, based on the evidence**

First, Doug’s act may be unethical, but possibly not against company policy. It seems like Santara hospital really needs to establish a corporate IT Usage Policy and it would have solved a number of problems, including this one. There are a lot of privacy issues with Doug taking his computer home because someone who should not have access privilege to the company records, could gain access quite easily.

Second, since a IT Usage Policy has not been in place, Cathy need to respond to Doug in a timely and professional manner before it is too late. Initially, Cathy should present the situation to her direct supervisor. Even though Cathy has been recommended as the head of the Task Force, she should still follow the corporate chain-of-command. If her supervisor does not take action, Cathy may discuss with him/her Cathy’s own plan to approach Doug in a meeting. If possible, Cathy should include her supervisor and HR Director in that meeting as well. She could begin by asking Doug how he has been utilizing his laptop after hours to determine if there is any potential risk. If he is not using it against company guidelines, the meeting will end. If Doug is saving confidential information directly to his laptop, Cathy may present a risk analysis of potential liabilities due to unsecured access to sensitive information. This will include all aspects, not just the specific risks involved with what Doug did (or may have done). Present real-life examples of information breaches to Doug and invite him to discuss the risks involved. The meeting records should be documented and presented a copy to HR to retain in Doug’s employee file.

**QUESTIONS RELATED TO THE CASE**

1. **Who are the key actors?**

Cathy, ER Director and Chief of the HIPAA Compliance Task Force; Doug, CFO; Cathy’s director supervisor; IT Director.

2. **What are the major issues in this case?**

A corporate executive’s off-the-hour usage of the company laptop computer and the information security risks may be involved.

3. **Is Doug violating the ethic code to put company’s mission-critical data and information at risk? Why or why not?**

Apparently Doug’s act is highly questionable and can be called unethical, but it is unclear that there is a company policy said that Doug cannot do so. Having the c-class access is critical and by not logging his computer, there could be high-level information security risks. Doug was also the person who issued the solution for patient record storage, as well as the CFO, so Doug should have known better. Nonetheless, as IT audit experts often point out, C-class executives in a corporation should resist the temptation to obtain more privilege in accessing, controlling, and changing mission-critical company information including documents, databases, and other intellectual properties (Brown-Schmidt, 2008).

4. **How would you approach Doug regarding the issue? In the process of dealing with the issue, how would you
involve your direct supervisor who reports to Doug? In detailed explanation including means of communication you choose.

Propose to call a meeting with the HR manager, my supervisor, and the Chief of Staff. Inform them of what is going on beforehand so they are aware of the situation. Have everyone voice the opinion on how Doug’s actions could negatively affect so many people not limited to the employees of the hospital but also the patients. By taking this avenue we are avoiding direct contact with Doug in case he takes this as a personal attack and tries to fire myself or any of my colleagues. This should also follow the hospitals procedure for the chain of command.

5. Would you do it differently if the problem is caused by employees at levels lower than that of Doug’s? How?

I would communicate directly with their direct supervisor and discuss the problem. I will then let their supervisor decide on proper actions/reprimands regarding the issue. Finally, I would inform the supervisor that information regarding this issue will soon be added to the operational procedures as well as the code of ethics.

6. What would you do to amend to the original technical upgrade plan on the laptop computers to reduce the risk of patient records being stolen?

(1) The following changes to the operational procedures as well as the code of ethics (Richardson, 2007):

- Enforce strict login/logout and password policies of technology assets.
- Enforce all laptops to be checked back in and/or scanned for problems after each logged out-of-site use.
- Install Deep Freeze on the local hard drives for all machines, not allowing editing or saving of files to happen. If machines are checked out for the night, they will not compromise security.
- On laptops and hand-held devices, require authentication to access any internal databases or network drives.

REFERENCES
