Georgia Hospital Association Compliance Officer Retreat

Privacy Case Study

Congratulations! It's your 1st day as the Chief Privacy Officer at the Ritz Hospital System. The Ritz Hospital System is a 1,500 bed hospital system that includes 5 hospitals, 2 ambulatory surgical centers, and 250 physician practices located in a major city in the Land of Peaches and Pollen. The Ritz's Chief Executive Officer meets with you and goes through a list of to-dos and recent health care privacy issues that have been brought to her attention over the last two weeks.

The List:

1. A member of your clinical staff took a photograph of a patient's injured leg and posted it on her private Instagram account. This patient is a well-known celebrity musician and has a tattoo of his initials and stage name on the injured leg (the initials and stage name are depicted in the photo). The clinical staff member's Instagram is private and she has no followers (*a follower can see the photograph on the user's account) except her best friend who works in a different unit at the Ritz Hospital.
2. A recently acquired physician practice staff's members share usernames and passwords to access patient accounts. This practice has a high turnover of employees.
3. An employee sent an email with an attached spreadsheet file that included 450 patient first and last names, date of birth, diagnosis, last 4 digits of the Social Security Number, their medical record numbers, and physician provider names to a patient in error. The email was opened but the attachment was not downloaded or opened on the patient's computer. This patient is a 1st year resident physician at a local academic medical center.
4. A Ritz Hospital clinician left medical record information for 10 patients on a desk at his second job at a local skilled nursing facility. These notes included the patients' full name, date of birth, diagnosis, and clinical updates. The desk is next to one of the nursing facility unit's shredder. The records are now missing.
5. A Ritz Hospital Business Associate (BA) Agreement expired/lapsed a year ago and the BA continues to provide services to the hospital. The Business

Associate has access to patients' financial information, date of birth, and social security number. Ritz Hospital has a contract with the BA and the BA performs monthly risk assessments and has a robust compliance/program.

6. A Ritz Hospital department who treats patients with sensitive health conditions has a department specific-practice of mailing a re-cap of patient visit summary information to their patients. The patients' name, date of birth, vitals, and diagnosis are listed on this one page summary. These summaries were placed in the incorrect patient envelopes. Fifty patients received the patient visit summaries for other patients.
7. The Ritz Hospital's Notice of Privacy Practices is listed on the website and posted in the patient waiting areas at each facility but is not actually handed/distributed to new patients.

Instructions:

As the Ritz's new Chief Privacy Officer, you will need to prioritize these privacy issues. Please rank these issues from #1-7. # 7 is high risk (should be resolved ASAP and controls should be implemented) and #1 is low risk (should be resolved but not as urgent). Please describe your rationale for ranking each risk on the number scale.

In the rationale, please answer the following questions for each issue:

1. Is this a privacy breach that the affected patient should be made aware of (through written notification)?
2. What controls, policies, or processes should be communicated or implemented?
3. What organizational resources should you ask the CEO for to mitigate these risks?
4. What Ritz Hospital departments should you work with to resolve these incidents/issues?