GRC Software Use Case for OCHIN, Inc.

February 8, 2016

ID:	Use Case 002
Title:	GRC software used to document investigations regarding an inappropriate disclosure of Protected Health Information (PHI)
Description:	Compliance Team reviews audit trail reports from the Epic Electronic Health Record (EHR) to determine if inappropriate access to PHI by an employee has occurred. The Same Last Name Report shows whether an employee has accessed his or her own medical record. The report also shows employees accessing someone with the same last name as themselves, possibly indicating that the employee is accessing a family member's medical record information.
Primary Actor:	Compliance Team.
Pre-conditions:	1. Employees receive medical care at the clinic that is also their employer. 2. New Employees and current employees receive HIPAA Privacy and Security training, which is documented in the Human Resources Information System (HRIS). 3. Employees sign a confidentiality agreement during their HIPAA training, which is maintained in the HRIS. 4. Clinic has written HIPAA privacy and security policies in place; these are located on the clinic Wiki page. 5. Clinic has an Employee Handbook that documents that PHI may only be accessed for work-related reasons. 6. Employees sign an annual acknowledgement indicating receipt of the Employee handbook, as well as HIPAA training. 7. Audit trails collect data about every view, access, change, or deletion of data from the EHR by a user. 8. On a monthly basis, the Compliance Team runs the Same Last Name Report and the Access Audit Report to determine if employees are accessing their own EHR, or that of a family member, or a fellow employee. 9. When an employee appears on the Same Last Name Report, it appears that the employee is accessing his or her own (or a family member's) EHR, the Compliance Team will investigate, including verifying with Human Resources (HR) whether the employee and the patient are the same individual, e.g. date of birth match, home address match, etc. 10. When an employee appears to be accessing other records inappropriately, the Compliance Team will investigate. 11. Compliance Team documents the findings from the Same Last Name Report review in the GRC software. 12. Compliance Team investigates the findings from the access reports to determine if inappropriate access has occurred.

	13. Compliance Team documents the conversation and information from HR about the employee who appears on the Same Last Name Report. 14. If the employee is confirmed to have accessed his or her own EHR, the Compliance Team verifies with HR that the employee has had HIPAA Privacy and Security training and documents that in the GRC software. 15. The Compliance Team verifies with HR that the employee has signed an annual confidentiality agreement and documents that information in the GRC software. 16. Compliance Team verifies that the HIPAA Privacy and Security policies are current and located on the Clinic Wiki page. 17. Compliance Team notifies the Integrity Officer about the findings and documents in the GRC software. 18. Integrity Officer notifies HR that the employee has violated company policy regarding accessing his or her own EHR and documents that information in the GRC software. 19. Integrity Officer contacts the employee's manager to give the manager information about the findings from the Same Last Name Report and from HR regarding the employee's access of his or her own EHR and documents that information in the GRC software. 20. Integrity Officer contacts the CEO, COO, and CTO to verify that a breach has occurred. 21. Integrity Officer contacts the CEO and the company legal counsel and provides information regarding the breach, with a request for review and recommendation. 22. Integrity Officer, HR Manager, and the employee's manager discuss the findings with the employee. 23. Integrity Officer makes a recommendation to the CEO, COO, the employee's manager, and HR regarding sanctions for the employee. This recommendation is documented in the GRC software. 24. Integrity Officer initiates the Breach Notification procedure, including notification to the patient, Office for Civil Rights, and other required individuals.
Post-conditions:	Compliance Team runs the Same Last Name Report and the Employee Access reports to determine if employees are accessing their own medical record, a family member's medical record, or a fellow employee's record, which is a violation of company policy.
Main Success Scenario:	Compliance Team maintains breach investigation and notification data.
Extensions:	Compliance investigations are maintained.
Frequency of Use:	Once per month
Status:	Currently maintaining this information manually
Owner:	Integrity Officer
Priority:	High