GRC Software Use Case for OCHIN, Inc.

February 8, 2016

ID:	Use Case 001
Title:	GRC software to maintain risk assessment documentation
Description:	On an annual basis, a HIPAA Privacy and Security risk assessment will be conducted and documented in the GRC software. Ongoing mitigation plan follow up will be documented in the GRC software.
Primary Actor:	Compliance Team
Preconditions:	1. Annually, the Compliance Team conducts a HIPAA Privacy and Security risk assessment using the risk assessment tool developed by OCHIN, Inc. 2. The risk assessment tool will be maintained in the GRC software. 3. A notice will be sent to the Compliance Team 90 days before the due date of the risk assessment notifying the team that the risk assessment is due in 90 days. 4. Each line item on the checklist has a link to the HIPAA regulation that must be complied with. Clicking on the link will open the Federal Register citation. 5. The risk assessment tool has linkages to the regulatory citations for each component of the tool. 6. The risk assessment tool has linkages to the relevant OCHIN privacy and security policies for each regulatory citation on the risk assessment tool. 7. Findings of compliance or non-compliance from the risk assessment are documented and maintained in the GRC software. 8. A mitigation plan is developed within the GRC software based on the non-compliance findings from the risk assessment, including plans to mitigate them. 9. The mitigation plan, and any progress that is made toward compliance with the regulatory requirements, is maintained in the GRC software. 10. If mitigation plans are not present for each area of non-compliance with the regulatory requirements, a notification will be sent to the department manager responsible for that compliance component requesting that they provide a mitigation plan. Notices will continue to be sent until a mitigation plan has been documented in the GRC software. 11. Department managers will document their mitigation plans within the GRC software for each area of non-compliance. 12. The GRC software will provide graphic representations of the progress for each non-compliant component of the risk assessment. The graphics

	will display data regarding compliance and non-compliance with the regulatory requirements, as well as the progress made on the mitigation plan for each area of non-compliance. 13. As regulatory changes to the HIPAA regulations are made, the risk assessment tool will be updated with the new requirement. 14. As regulatory changes to the HIPAA regulations are made, a notice will be sent to the Compliance Team, notifying them of a change, including the link to the regulation.
Post conditions:	1. The GRC software will provide graphical information about the areas of compliance and areas of non-compliance at OCHIN. 2. The GRC software will provide graphical information about the progress made on the mitigation plan for each area of non-compliance. 3. Managers needing to document mitigation plans for areas of non-compliance are sent reminders about missing documentation until the documentation has been completed. 4. As regulatory requirements that are changed, the GRC software will update the risk assessment tool with the new requirements.
Main Success Scenario:	Notice of risk assessment is sent to the Compliance Team 90 days before the risk assessment is due. Annual risk assessment findings data is documented. Mitigation plans for areas of non-compliance that were determined during the risk assessment are documented. Current compliance status is displayed graphically. Progress on mitigation plans is displayed graphically.
Extensions:	Risk assessment calendar will document the risk assessment interview schedule.
Frequency of Use:	Risk assessment will be annual. Mitigation plan and follow up will be on-going.
Status:	Currently maintaining data in Excel
Owner:	Compliance Team
Priority:	High