Director, HIPAA Security & Risk Management Director, HIPAA Security & Risk Management Director, HIPAA Security & Risk Management (Remote) McKinney, TX Analyzing, auditing and consulting on processes in support of operational excellence, the achievement of business objectives, and performing risk assessments. Expert in managing multiple assignments, and delivering desired results ahead of schedule. Professional ability to develop positive working relationships with clients and colleagues at all organizational levels. Excellent research skills, with clear and concise writing ability. Relationship driven service professional that can solve problems and maintain relationships. Work Experience Director, HIPAA Security & Risk Management NFP (Remote) August 2015 to Present Complete annual HIPAA Risk Assessments that identify current and future internal and external information security vulnerabilities, provides necessary information about risk acceptance and risk mitigation, and coordinate with departments to identify strategies to reduce information security risks. Identify company information assets including hardware, platforms, servers, emails, or anything that connects through internet access, data in transit, and data at rest. Collaborates with appropriate departments to ensure that HIPAA related policies and IT controls are being effectively developed, implemented and executed. Performs ongoing security compliance monitoring activities as needed for firms that have ePHI. Conduct research in an effort to keep up to date with new compliance rules and applicable regulatory changes as it pertains to HIPAA Security and Privacy Rules for ePHI. Work with IT and IT Audit on examining and analyzing the information system operations to identify opportunities for risk reduction for ePHI. Ensure the appropriate level of information security is utilized based on industry standards, best practices, HIPAA, and other regulations by developing repeatable processes to identify, evaluate, and measure security risks for ePHI. Assist in reviewing HIPAA security policies, procedures, and standards. Manage the remediation for HIPAA security review findings and recommendations. Information Security Analyst - Risk Management Capital One (Remote) March 2015 to July 2015 Provide operational support for Information Security's program to ensure compliance with FFIEC Guidance on Multi Factor Authentication in an Internet Banking Environment. Perform annual risk assessments, identifying/documenting gaps in meeting a defined set of requirements, and tracking

open vulnerabilities/compliance gaps. Executing the annual risk assessments of all in scope platforms including web, VRU and call center groups leveraging established procedures and tools. Worked in RSA Archer GRC tool. Perform penetration Web application testing for banking environment. Documenting functions, capabilities, authentication processes, and layered security controls for electronic banking applications. Identifying and tracking findings from completed risk assessments leveraging established procedures. Information Security Compliance Analyst Torchmark Corporation January 2014 to March 2015 Research, analyze business functions, processes, documentation and requirements to be in compliance with PCI, HIPAA/HITECH, GLBA, Part D, EU/EAA, NACHA and other regulations that relate to Information Security, Compliance and Privacy within the organization. Assess privacy, security or compliancy breaches and/or leaks with Data Loss Prevention Tool with DLP incidents, Data at Rest and the remediation. Assist defining business requirements and or business process solutions with the Business Units of the organization. Work with Business Units on data classification, retention, and deletion requirements, data loss prevention. Manage continuous monitoring process development and integration with existing processes, including security control assessment, and risk management. One of the Team Leads in GRC software tool for Compliance Regulations, assessments, and assigning workflows to appropriate Business Units. Perform computer security audits, and user audits reviewing application and operating system user access controls. IT Security and Compliance Systems Analyst CVS July 2013 to December 2013 Responsible for execution and monitoring of activities focused on maintaining compliance with CVS Caremark Internal policies and regulatory compliance; Accountable for executing all activities in support of periodic access review compliance.

Worked in RSA Archer GRC tool. Responsible for performing periodic access reviews on systems and applications to validate user and system id access, primarily focusing on security administration. Perform web based application penetration tests and assessments. Responsible for acting on security violations. Work on multiple platforms, technologies and projects as a team member and leads data-related security components maintained by Enterprise Software. Work independently or on multiple IT security projects as project team member, occasionally as project

leader. Prepare remediation plan and work with teams to ensure remediation is completed on time. Maintain evidence as defined by corporate policy. Provide support in maintaining inventory of key assets namely systems and critical libraries. Effectively communicate and partner with large number of teams, across various geographical locations to minimize risks and stay compliant. Coordinate and identify critical libraries and support monitoring of identified assets. Provide operational metrics and reports on assigned tasks. HIPAA, PCI, and PHI compliant. Perform computer security audits, and user audits reviewing application and operating system user access controls. Client Analyst Large Group (Consultant) HUMANA (Remote) March 2013 to July 2013 Review & prepare all sold case processing. Interact with clients, brokers, and associates to provide the highest possible level of service. Act as an in-office resource to Brokers, securing rates, reviewing cases and securing missing information and processing new business groups and renewals. Review proposals, new business quotes, and rate sheets. HIPAA, PHI compliant. Implementation Data Analyst, Sales Development Group (Consultant) BLUE CROSS BLUE SHIELD (Remote) June 2012 to January 2013 Researched, analyzed and gathered data to support the implementation of new or renewing accounts, new legislation, and products across the enterprise. Works with cross functional teams/internal stakeholders, project management office to coordinate implementation. Responsible for communications and implementation artifacts that describe progress, issues, and risks surrounding the implementation. Responsible for assisting with managing implementation project activities of low to moderate complexity. Gathering, organizing, analyzing, and interpreting marketing, legislative, financial, and operating data. Keeps informed of best practices and strategic trends in product lifecycle management, sales and account implementation, and legislative developments. Microsoft Excel for importing and exporting reports.

MS Access database utilized. Education Business Administration Southwestern Illinois College Skills Sharepoint, Rsa, Ms access, Oracle, Crm, Excel, Ms excel, Lotus notes, Ms outlook, Outlook, Ms word, Word, Risk Management, Compliance, Governance, Risk Management, Governance, Compliance, Internal Audit Additional Information TECHNICAL SKILLS: Oracle CRM MS Word, MS Excel MS Power Point, MS Access MS Outlook Lotus Notes SharePoint Lockpath GRC RSA

Archer GRC Egnyte Salesforce Clearwater Compliance

Name: Jaclyn Lee

Email: eyoung@example.com

Phone: +1-970-603-3083x663