IT Security Policy Analyst IT Security Policy Analyst IT Security Policy Analyst Woodbridge, VA As experienced Information Assurance (IA) and compliance officer, I look forward to staying on the cutting-edge of Cyber Security trends as I progress throughout my career.   Skills/ Technical Tool   System Life Cycle Project Management (SDLC)   Security Assessment & Authorization   System Security Documentation   POA&M & Vulnerability Management   Cloud Computing Security   Risk Management Framework (RMF)   NIST 800 series   FISMA and FedRAMP   Professional Profile * Achieved and maintained %100 compliance with consistent "green" status, applying my skills in federal security policies, standards, and procedures including NIST 800 SP's such as 800-37, 800-60, 800- 53/53A rev 4, FIPS 199/200, FISMA, OMB, ISO & FedRAMP. * Thorough knowledge of Risk Assessment, Risk Management Framework (RMF), Systems Development Life Cycle (SDLC) and Security Assessment and Authorization (A&A) process. * Development, review, implementation and auditing of System Security Plans (SSP), Contingency Plans (CP), Disaster Recovery Plans (DRP), Incident Response Plans (IRP), and Configuration Management Plans (CMP) and Plan of Action and Milestones (POA&M). * Implementation and audit of Privacy Threshold Assessments (PTA), Privacy Impact Assessments (PIA) of sensitive IT systems and security processes and procedures. * Collaborative interaction with multiple, internal and external stakeholders: interviewing, planning and participating in a team effort to bring multiple complex projects to execution in highly motivated environment. * Excellent leadership, teamwork, and client service skills. Thrive in a highly collaborative, fast-paced work environment and multidisciplinary team setting where leveraging technology for continuous business improvement is the norm. Work Experience IT Security Policy Analyst Circle of Hope Therapeutic Services Inc - Springfield, VA September 2017 to Present   Help with Health Insurance Portability and Accountability Act (HIPAA) framework implementation as it relates to guidelines, standard and privacy requirements   Review, interpret and train staff on policies and regulations, specifying the impact on the community, agency, workers and clients, while further ensuring the proper application of policies and regulations per requirements   Ensure that all identified deficiencies from vulnerability scans are addressed in a Plan of Action and Milestones (POA&M), track remediation actions and report status to senior management Conduct a comprehensive assessment of the management, operational, and technical security controls employed within or inherited by systems to determine the overall effectiveness of the controls implemented Responsible for conducting security Assessment and Authorization (A&A) activities using industry standard frameworks such as NIST, FISMA, RMF, and HIPAA Give advice, recommendations, guidance to program management and insight into the overall management and evaluation of the system security posture including migration of systems to the cloud Participates in appropriate level of response, develops corrective action plans, and oversees compliance investigations while maintaining confidentiality of information reported, as appropriate Investigate system security incidents to determine the extent of compromise to information systems Ensure information systems are assessed, integrated, accredited, operated, maintained and disposed of in accordance with applicable security policies and practices outlined in Standard Operating Procedure (SOP) and customer directives Develops and monitors programs, policies and procedures to ensure compliance with applicable federal and state laws and regulations, such as those for Medicare, Medi-Cal, third party payers, and other related public healthcare programs Information Assurance Analyst North Capitol Collaborative Inc - Washington, DC December 2016 to June 2017 Supported threat management and security incident handling program that aligned patient needs and regulatory requirements with our compliance objectives Created and maintained required security artifacts such as Contingency Plans (CP), Incident Response Plans (IRP), and MOUs/ISAs Performed periodic attestation, control, and performance procedures as deemed necessary Worked collaboratively with respective stake holders to ensure efficient service delivery, evaluated effectiveness of program outcomes, and developed new intervention strategies Provided leadership, direction, and development and implementation of strategic initiatives to improve and enhance performance and services Used a variety of information applications and databases to develop schedules and special reports Reviewed inquiries concerning billing and documentation, reports of noncompliance and results of documentation compliance audits and makes recommendations regarding corrective actions Information Assurance Analyst National Counseling Group (NCG) January 2016 to December 2016

Ensured security, maintenance and management of medical records of clients in order to meet the HIPAA requirements Carried out analysis and update records of incident, issues and risk registers Coordinated various compliance activities with other departments, outside vendors and service providers to achieve programmatic compliance with applicable rules and regulations Responded to a variety of information requests from both inside and outside the agency Developed and monitors policies and procedures that establish standards for ensuring client privacy protections, including by providing guidance to individual employees and departments on the HIPAA Privacy Rule, as appropriate Quality Assurance Analyst Piedmont Geriatric Hospital- Department of Behavioral Health and Developmental Services - Burkeville, VA September 2014 to August 2015 Conducted IT risk assessment and documented key controls. Prepared and reviewed A&A package for information systems. Evaluated, tested, recommended, monitored and maintained information assurance controls. Analyzed and defined security requirements for networks, application/systems, end user computing, mobility and data center solutions. Developed security standard and procedures as well as conducted vulnerability analysis and risk assessment. Participated in health and hospital related compliance program studies and projects Performed audits to assess compliance with various laws, regulations, policies and standards such as those related to health care fraud, waste and abuse, billing, clinical documentation, privacy and information security, research, and ethics Education Masters of Social Work in Psychology Clark Atlanta University - Atlanta, GA Skills Security, training, testing, access Certifications/Licenses CompTIA A+ Certified Scrum Master

Name: Brittany Taylor

Email: matabilly@example.com

Phone: 6708077825