NICOLE D. SCOTT

SUMMARY

A certified compliance, ethics, and cybersecurity expert with vast experience in the creation, implementation, and management of cybersecurity and compliance programs including the required privacy, security, and operational policies and strategies to ensure compliance with their legal and regulatory obligations while promoting integrity.

EXPERIENCE

ISMIE Mutual Insurance Company, Chicago, Illinois
Vice President of Compliance l Chief Information Security Officer l Asst HIPAA Privacy Officer, HIPAA Security Officer (01/2023-Present)
AVP of Compliance l Chief Information Security Officer l Asst HIPAA Privacy Officer, HIPAA Security Officer (2020 to 2022)
Director of Operations Compliance (2018 to 2020)

- Develop, implement, manage, the Companies' Compliance Program and Cybersecurity Program.
- Oversee and manage enterprise-wide governance initiatives, including enterprise policies and information management.
- Develop and implement the security policy management strategy.
- Provide direct reports, guidance, and training to the Board of Directors and Senior Executives on Compliance and Cybersecurity activities.
- Establish policies, procedures, and written Data Security Plan to ensure compliance with HIPAA, HITECH, privacy laws, and NAIC data security laws.
- Oversee the Cybersecurity Program to maintain the integrity and security of the Company's data and systems to meet or exceed security best practices.
- Direct the IT security strategy and architecture plan.
- Plan for the deployment of security technologies.
- Communicate with the Board and key stakeholders about IT security threats, status, and compliance.
- Drive technology transformation through the selection and management of systems to the cloud.
- Respond, investigate, and mitigate data security incidents, breaches, and regulatory requests.
- Develop and administer the IS Risk Assessment from concept to implementation.
- Partner across the business, technology, and the executive leadership to respond to enterprise risk assessments and compliance and regulatory audits.
- Train and educate on policies, procedures, and security strategies and technologies.
- Facilitate activities necessary to protect corporate integrity and ensure compliance with all regulatory requirements, policies, and procedures.
- Identify trends and potential areas of compliance and data vulnerability and develop and implement corrective action.
- Create, administer, and manage the Enterprise Wide Risk Management Assessment.
- Create, implement, and manage the Companies Third Party/Vendor Management Program from concept to implementation.
- Lead and manage Department of Insurance Examinations and External Cybersecurity Audits.

ISMIE Mutual Insurance Company, Chicago, Illinois
Professional Liability Specialist, Medical Malpractice Litigation Management (2004 to 2018)

- Negotiate settlements in excess of 10 million dollars.
- Provide training on legal concepts, new system integration and internal process changes.
- Evaluate and allocate liability and indemnity estimates on an average caseload of more than 100 medical malpractice claims totaling more than $75 million in open exposure.
- Recommend defense/settle posture and execute until resolution of the case.
- Organize, review, and summarize medical records, depositions, case law and legal doctrines.
- Manage the unexpected outcome program including 24 hour claim handling, direction, and coordination of real time liability exposures.

GENERAL ELECTRIC-AIRCRAFT ENGINES, EVENDALE, OHIO
Law Clerk, Labor and Employment Legal Division (2003 to 2004)

- Researched and analyzed potential liability involving with ADA, FLSA, FMLA, EPA, NLRA, WARN, ADEA, and Title VII.
- Evaluate Corporate Compliance, Union and Management Governance, and NLRB policies in an effort to reduce potential litigation and claims.
- Drafted official company position statements for federal agency (EEOC, NLRB) charges.
- Assisted in Collective Bargaining Preparation and Strike Preparedness for negotiations covering over 10,000 represented employees.

SOUTHERN OHIO REGIONAL TRANSIT AUTHORITY, CINCINNATI, OHIO
Law Clerk, General Counsel and Human Resources Director (2001 to 2002)

- Researched analyzed potential liability involving FMLA, EEOC, ERISA, and those concerning Human Resource Compliance.
- Evaluate potential liability from Union and Corporate Management Relations.
- Investigated compliance with Non-Political governmental entity regulatory requirements.
- Drafted Employer/Employee Court Ordered & Private Settlement Agreements.
- Participated in arbitration procedures in place of or in support of the general counsel.
- Created Human Resources Policy and Practices

EDUCATION AND TRAINING

May 2004 — **J.D. Corporate Law**
UNIVERSITY OF CINCINNATI COLLEGE OF LAW - CINCINNATI, OHIO

May 2003 — **Masters of Business Administration**
UNIVERSITY OF CINCINNATI COLLEGE OF BUSINESS - CINCINNATI, OHIO

May 2000 — **Bachelor of Arts- Business Administration and Political Science**
ILLINOIS WESLEYAN UNIVERSITY - BLOOMINGTON, IL

CERTIFICATIONS

August 2018 — Certified Compliance & Ethics Professional (CCEP)
Society of Corporate Compliance and Ethics (SCCE)

March 2019 — Certified in Healthcare Privacy Compliance (CHPC)
Health Care Compliance Association (HCCA)

PUBLICATIONS

2019- Present — Co-Editor for the Illinois Association of Healthcare Attorneys (IAHA) Annual Survey of Health Law.

2020-Present — Book Chapter, "*The Law of Medical Practice in Illinois*", updated annually (West Group, 2020 Edition).

ADDITIONAL SKILLS AND EXPERIENCE

- Experienced in leading business, compliance, and comprehensive cybersecurity programs in a highly regulated environment.
- History of leading and monitoring information security, cybersecurity, and technology risks across the organization, its affiliates, and third parties.

- Ability to recognize gaps in operations and processes and recommend holistic solutions.
- Experienced in security transformations driving change to cloud and cloud-enabled solutions.
- Effective in influencing and negotiation abilities.
- Strong interpersonal and advocacy talents.
- Proven history of leading diverse groups at all levels of the organization to achieve a culture of regulatory and cybersecurity compliance.
- Coordinated with business partners to influence security initiatives across the enterprise and find opportunities to align those initiatives to the business strategies.
- Unquestioned integrity and professional maturity.
- Experienced in developing and implementing compliance and cybersecurity programs.
- Superior written and oral communication skills.
- Developed long term strategies to mitigate key threats and risks, while managing improvement through program and process execution.
- Advanced change management skills.
- Facilitated a culture of compliance and cybersecurity awareness.
- Proven ability to work in a cross-functional environment without direct authority.
- Delivered innovative and effective solutions to address growing cybersecurity and privacy demands.