



Gorman Consulting (<https://gormanconsulting.org>) is a firm that provides specialized measurement and evaluation services, primarily in the health sector. We are working with laboratories around the world to compile and standardize clinical and pre-clinical results from COVID-19 vaccine trials. We are seeking a data security consultant to assess the design of our ETL workflow, our cloud application hosted on Heroku, our PostgreSQL database, and our overall business processes to ensure 1) compliance with GDPR/HIPAA and 2) that the systems are ready for penetration testing.

Responsibilities

- **During the design stage of the ETL workflow and data warehouse containing personal biomedical data, advise on all aspects of the structure and pipeline to ensure compliance with GDPR/HIPAA and all regulatory submission requirements.** The consultant will serve as the subject matter expert for data protection laws. Example tasks include ensuring the security of the data storage and retrieval systems as well as data anonymization and encryption processes; creating incident management protocols; ensuring user permissions are sound and in line with laws and best practices; setting up our Security Information and Event Management framework.
- **Review our data security policies and operational procedures to advise on where to strengthen.**
- **Ensure our systems are ready for penetration testing.** The testing will probe for design and/or functionality weaknesses in applications, network perimeters, or other infrastructure elements as well as weaknesses in process or technical countermeasures relating to Gorman Consulting's Information Systems. The consultant will identify and provide recommendations for any identified security vulnerabilities including: invalidated or un-sanitized input; broken access control; broken authentication and session management; cross-site scripting (XSS) flaws; buffer overflows; injection flaws; improper error handling; insecure storage; denial of service; insecure configuration management; proper use of SSL/TLS; proper use of encryption; and anti-virus reliability and testing.
- **Help identify a firm to perform penetration testing and assist with incorporating any results, as helpful.**

Qualifications

- A Degree or Diploma in Computer Systems, Computer Security, or another IT related discipline. Professional certifications such as OSCP, CISA, CISSP/CISM, ISO/ICE 27001/2 Auditing, preferred
- Proven track record with data security in high profile environments, including at least 5 years of experience in IT security and ensuring compliance with data protection laws; candidates with experience with vulnerability assessments will be prioritized.
- Expertise in global and European data protection laws and practices and an in-depth understanding of the GDPR required; Comfort with HIPAA, GxP quality control guidelines and Title 21 CFR Part 11.
- Experience implementing security measures on cloud platforms such as Heroku, AWS, Azure and Google Cloud Platform; Experience in SIEM (Azure Sentinel) and Threat Intelligence preferred
- Strong critical thinking skills and meticulous attention to detail. For example, use the subject line "Application for Data Security Consultant: *Your Last Name*" in your email application.
- Strong written and verbal communication skills.

To apply, send your CV to jobs@gormanconsulting.org. Only shortlisted candidates will be contacted. Candidates must have legal authorization to work within the country they are based.