Center for Improving Value in Health Care (CIVHC)
JOB DESCRIPTION

Position Title: Compliance and Data Privacy Officer
Reports to: VP of Innovation and Compliance
Job Classification: Exempt, Full time

The Center for Improving Value in Health Care (CIVHC) is a growing health care data nonprofit. CIVHC administers the Colorado All Payer Claims Database (CO APCD) for the state, and supports consumers, providers, employers, researchers, state agencies, communities and others with data and analytics to drive improvements in health and health care. We are seeking a Compliance and Data Privacy Officer to lead our health care data compliance work which includes evaluating appropriate uses of the data, managing data audits, ensuring internal adherence to federal privacy and security laws, and permissible uses of Medicare data.

We are looking for an individual who is passionate about CIVHC's mission to advance the Triple Aim of improving health, improving quality and lowering costs, and has experience working with data compliance issues in large datasets. To succeed in this role, you should be a reliable professional who is not afraid to speak their mind and stand by their decisions. You should be familiar with risk management and health care industry standards. CIVHC is a creative and collaborative environment and we are looking for a team member who is eager to figure out how we can most effectively support our stakeholders. This position will report to the Vice President of Research and Compliance, and will work closely with the Vice President of Data and Analytics and the analytic team to develop and manage the data privacy governance across all of CIVHC's work portfolio.

Responsibilities:

- Build and maintain CIVHC's privacy and information security programs, including upholding the organization's policies and procedures, designing and implementing training and education programs, and being the subject matter expert on privacy and information security requirements.
- Stay up to date on changes to federal data policy, including HIPAA, HITECH, ERISA, 42 CFR Part 2, antitrust guidance, and others. Update CIVHC internal data policies and procedures to reflect current law.
- Ensure internal and external (public and non-public) reporting is compliant with federal and state privacy laws, that CMS suppression guidelines are met, and there is no risk of re-identification of individuals or reverse engineering of reimbursement to individual providers.
- Act as point person for all stakeholder privacy and security concerns.
- Manage external data use compliance through CIVHC's Data Release Review Committee (DRRC), including reviewing applications for data and analytics, facilitating DRRC meetings and guiding the committee's review of applications. When the DRRC recommends changes to a data request application, communicate recommended changes to the data requestor. Conduct any follow up with requestors to bring requests into compliance with all applicable privacy laws and policies.
- Create policies and procedures for internal compliance review for projects that do not need full review by the DRRC.
- Be primary contact for federal data use and access, including Medicare fee-for-service claims and any other data CIVHC may obtain from federal sources to supplement the CO APCD.

- Build and maintain CIVHC's privacy and information security programs, including upholding the organization's policies and procedures, designing and implementing training and education programs, and being the subject matter expert on privacy and information security requirements.
- Conduct audits of data destruction certificates from past clients and ensure adherence to the terms of Data Use Agreements.
- Review and approve data requests from external CIVHC data holders. Receive and file annual report listing all related data requests.
- Become the subject matter expert on CIVHC's Qualified Entity status, including ongoing reporting of Medicare data use to CMS, requesting data refreshes, and communicating with the state of Colorado on uses of Medicare data.
- Other duties as assigned.

Requirements:

- Bachelor's degree in a related field; Master's degree preferred.
- 5-7 years' experience in health data privacy and compliance.
- Healthcare Privacy Compliance certification from a reputable association is strongly preferred.
- Thorough understanding of health care data and privacy requirements, as well as relevant antitrust concerns. Familiarity with HIPAA de-identification requirements and CMS Medicare data standards preferred.
- Experience with data governance and the management of regulated data.
- Responsible, detail oriented personality.
- Able to comfortably read and interpret state and federal regulation, and stay abreast of legal developments and changes.
- Team player, comfortable collaborating with others and training peers on compliance requirements.
- Excellent communication and writing skills.
- Comfort with legal terminology and contract review preferred.
- Positively represent CIVHC at local and national events.

Preferred Qualifications:

- Experience with health care claims data.
- Familiarity with the health care insurance industry.

Physical Requirements:

- Ability to work at a computer for extended periods.
- Ability to travel to and from meetings locally and potentially occasional overnight national travel.

CIVHC is an equal opportunity employer.

Limitations and Disclaimer:
The above job description is meant to describe the general nature and level of work being performed; it is not intended to be construed as an exhaustive list of all responsibilities, duties and skills required for the position.

Application Instructions:
Interested candidates may submit cover letters and resumes to careers@civhc.org. Please include the job title and your name in the email subject line.