Position Brief for the position of Chief Privacy Officer
Stanford University
February 2019
Contents

Opportunity Overview 3
About Stanford University 4
The Position 5
The Candidate 9

Contact Information

Kathryn Ullrich | Partner, Technology
O: +1 650-567-5035
M: +1 415-902-6756
kathryn.ullrich@odgersberndtson.com

Monica Burton | Partner, Education
O: +1 646 430 9906
M: +1 651 247 4507
monica.burton@odgersberndtson.com

Odgers Berndtson

Silicon Valley
951 Mariners Island Boulevard, Suite 300
San Mateo, CA 94404

New York
750 Lexington Avenue, 10th Floor
New York, NY 10022
Opportunity Overview

Stanford University, one of the world’s preeminent institutions of higher education, seeks a seasoned, innovative leader to serve as the University’s Chief Privacy Officer (CPO). This is a unique opportunity to work in a truly entrepreneurial academic community to steer and enhance an effective privacy program, and, in turn, advance Stanford’s leadership presence in this realm.

Reporting to the Senior Associate Vice President and Chief Risk Officer (CRO), the CPO will provide proactive direction, guidance, and support to administration, faculty, and staff in all aspects of privacy for the University. S/he will ensure the protection of information entrusted to the University related to students, faculty, administration and staff, research participants, and other key constituents.

While managing the organizational risk associated with privacy, the successful hire will enable innovation and discovery related to data. The CPO will be expected to: ensure all aspects of privacy are protected across the University while promoting academic freedom and enabling innovation; cultivate and leverage robust collaborations with key partners on campus and across the Stanford ecosystem; increase awareness and proficiency around privacy issues that reduce risk and infractions; build, mentor, and develop the Privacy team; and represent Stanford effectively in external venues.
About Stanford University

Stanford University, founded in 1885, today comprises seven schools and 18 interdisciplinary institutes with more than 16,000 students (7,000 undergraduate and 9,000 graduate), 2,100 faculty, 1,800 postdoctoral scholars, and over 12,000 staff. Stanford is an international institution, enrolling students from all 50 U.S. states and 91 other countries, and with education and research activities with 125 global entities.

The university’s annual revenue is approximately $6.5 billion (exclusive of affiliated hospitals) including $1.6 billion of research funding; the endowment as of 8/31/2018 was $26.8 billion dollars, one of the largest in the country.

Lucile Packard Children’s Hospital and Stanford Health Care are affiliated entities of Stanford University, and combined with the School of Medicine, comprise Stanford Medicine.

See the following links for more information:
- Stanford University [https://facts.stanford.edu/](https://facts.stanford.edu/)
- School of Medicine [http://med.stanford.edu/](http://med.stanford.edu/)
- Stanford Health Care [https://stanfordhealthcare.org/](https://stanfordhealthcare.org/)
The Position

Residing in the Office of the Chief Risk Officer (OCRO) and reporting to Rick Moyer, the Senior Associate Vice President and CRO, the CPO is an expert on privacy matters related to large complex, customer-oriented, research-intensive organizations entrusted with large volumes of sensitive, confidential data of a critical nature to the enterprise and its constituents. S/he is an exceptional leader, digitally proficient with sound business judgment, who can set the strategy, navigate the complex and changing landscape of regulatory compliance, and innovate to drive a world class privacy platform that is a fundamental institutional value and priority.

Overview of the Privacy Office (PO)

With a staff of five, the CPO leads the Privacy Office (PO) in the further implementation, coordination, and management of a comprehensive privacy program to meet state, federal, and international laws, regulations, and rules regarding privacy. The PO is one of six departments within the OCRO. Peer organizations to the PO are: Enterprise Risk Management (ERM), Internal Audit Services, Ethics and Compliance, Risk Management and Information Security (which reports dually to University IT.)

Primary functions and objectives

The PO is expected to identify and develop initiatives to prevent, detect, and respond to internal and external privacy risks through the construction and maintenance of a comprehensive privacy plan, policies and procedures, annual auditing and monitoring plans, and privacy education and training for Stanford University.

Protection of confidential data

Safeguarding members of the Stanford community, the PO helps these organizations accomplish their objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and government processes. The PO establishes and maintains practices to protect personal and institutional information in a manner consistent with University values and applicable laws and regulations. The group is expected to anticipate and address privacy issues as they arise, responding to both internal and external inquiries, concerns, and complaints, and prepare formal responses.

Staying current and being proactive in the dynamic regulatory environment

Ensuring Stanford complies with applicable state, federal, and international laws, University policies and procedures, and privacy standards, the PO is also expected to provide early warning services to the entire campus regarding new regulations or privacy initiatives by government or regulatory agencies, in coordination with appropriate stakeholders and partners.
Training and guidance of faculty, staff, and students
Committed to working with parties across the Stanford community to protect the integrity of data collected, created, transmitted, released, and stored by Stanford affiliates and entities, the PO works with stakeholders throughout the Stanford community to provide training, guidance, and consultation in furtherance of the University’s mission, and applicable privacy laws and regulations.

Investigations and responses to privacy incidents
Members of the PO will conduct investigations as needed and follow cases thoroughly to resolution. In these investigations, a member or members of the group will take the lead into investigating allegations of privacy violations, resolve any issues, and strengthen operational controls to ensure that program components and activities meet and exceed state, federal, and international privacy laws in addition to the Office of Civil Rights (OCR) guidance.

Working in tandem with Stanford Hospitals and coordination with School of Medicine
While there is a separate Office of Compliance and Privacy for the Stanford Hospitals, these offices and individuals within them work together very closely. The School of Medicine and Stanford Hospitals share practitioners and faculty so incidents and implementations of new practices within the medical space require coordination across the University and Hospitals. Both offices work to address privacy issues such as those related to electronic health records (EHR) policies and procedures, the release of information, electronic media development, application of relevant laws and regulations, filing of complaints about privacy practices, maintenance and dissemination of the notice of privacy practices, and appropriate activities of volunteers, visitors, vendors, observers, and trainers.

Partnering with and leveraging the Office of the General Counsel (OGC)
The Office of General Counsel (OGC) and the PO must work closely to ensure success. As the topics in the privacy realm cover a considerable range, expertise of the OGC will be instrumental in addressing new and complex incidents. Success in the role of CPO is reliant on a coordinated and developed partnership with University Counsel.

Supporting board communications
In addition to working with the CRO in preparation to speak with the Board, the CPO will be the PO’s lead representative in making presentations regarding privacy issues to the University’s Board of Trustees Audit, Compliance, and Risk Committee as well as the Executive Privacy Governance Council (EPGC).

Information security best practices
While the CPO is not responsible for the technical aspects of security, s/he will work with the Chief Information Security Officer and the staff of the Office of Information Security to ensure policies and procedures, incident response, and other provided services are utilizing best practices and new technologies, and the two offices are coordinated in their messaging.
Key Opportunities and Challenges

In addition to ensuring effective and seamless execution of the objectives of the PO, the CPO will face the following opportunities and challenges:

**Proactively managing privacy risk, ensuring academic freedom, and enabling innovation**

The CPO will build programs that will increase awareness of privacy issues in all aspects of the campus' operations; enhance and develop mechanisms to successfully protect access to information, data, and records; and ensure compliance with established and new policies and procedures. This will be accomplished without thwarting academic creativity, academic freedom, and enterprise innovation.

While the ultimate goal is to protect the University, the PO should be approachable, proactive, and creative. As an example of the duality of the role, the CPO and his/her staff are expected to be active in investigations while developing the policies and procedures that prevent the need for such reactive activities. S/he must steward a comprehensive privacy plan for response and preemption, continuously developing standards to measure the program's effectiveness, and communicating that plan to key partners in a way that is pragmatic and respectful of the realities of operating in an intellectual porous and creative environment.

The CPO will balance the conflicting objectives of the Hospitals and other entities that have vast amounts of data who are bound to protect the privacy of the data, while upholding the research objective of the University with faculty and researchers who need to leverage this data in their research studies. The CPO will work toward finding solutions to meet research needs while protecting privacy.

It will also be a delicate and important balance to respond to incidents as they arise, while developing a proactive culture of privacy on campus. The CPO must stay abreast of best practices and current legislation and write strong rules and regulations that reflect those practices. Because the work at Stanford, especially clinical and research work, often extends beyond the walls of any one department into multiple areas, the CPO must ensure the education and training of key stakeholders and the maintenance of the privacy regulations across the University.

**Cultivate and leverage collaborations with key partners on campus**

The OCRO member units work closely together as they have many points of intersection and overlap. Not only must the CPO build and develop his/her staff, but s/he must work closely with the staff and leaders of OCRO to maintain service excellence while meeting organizational goals.

Beyond OCRO, the CPO maintains close working relationships with the University’s senior operating management to coordinate strategy and develop privacy policy, including the OGC, the Information Security Office, the Student Services Center, the University Human Resources Benefits Office, research offices, and the Hospitals’ Compliance and Privacy Office. S/he will capitalize on the vibrant spirit of
partnership across campus cultivating, developing, and managing these internal relationships, and work collaboratively with key partners in implementing the University’s privacy policies and procedures campus-wide. These partnerships will ensure privacy considerations are part of every University project and/or initiative, privacy-related risks are mitigated, and the Privacy Office is a key player in the University’s data governance activities.

**Build, develop, mentor and promote world class Privacy team**

Taking the view of that of an “orchestrator,” the CPO must manage, delegate, mentor, and give agency to team members in order to foster a premier privacy program that will be at the forefront of programs nationally. In addition to creating and executing short- and long-term strategic plans for the department's success, the CPO must think strategically about the development and growth of the team as a whole as well as its individual members. Strategic hiring, professional development of team, and professional guidance and mentorship are critical functions of the CPO role. A key will be hiring a Deputy Privacy Officer and developing a succession plan amongst the team. Under the CPO’s expert leadership, the PO at Stanford will be a model for innovation and the effective risk management of critical data.

**Represent Stanford effectively in external venues**

As part of the CPO’s public role, s/he will provide leadership in representing the University in relevant national organizations. With the success of the University’s privacy programs, it will be natural for the CPO to participate in and/or lead the national conversation in the academy around privacy issues and solutions, a role that Stanford executives often play in their respective fields.
The Candidate

Ideally the successful candidate will bring most, if not all, of the following professional qualifications, characteristics, skills, experience, and personal qualities:

- Ten or more years of increasingly responsible privacy management experience in a large research university, academic medical center, or other relevant complex organization. Digital proficiency, sound business judgment, and an understanding of privacy in healthcare are critical. Success operationalizing a privacy program is ideal;

- Ability to understand, research, analyze, interpret, and apply complex federal, state, and international privacy laws, rules, regulations, and guidelines and the constantly changing risk profiles and evolution.

- Demonstrated success in training and educating a range of stakeholders on a comprehensive privacy plan as well as active and appropriate responses to different incidents and investigations;

- A thorough understanding of industry best practices in privacy and demonstrated success in strategic planning, program evaluation, and improvement to create and implement a vision for privacy operations.

- Ability to foster a culture that encourages awareness of privacy and ensures compliance with established policies and procedures across campus.

- Dedication to treating both internal and external constituents as clients, maintaining a flexible customer service approach and orientation that emphasizes service satisfaction and quality;

- Demonstrated ability to build successful relationships with a wide range of staff across a complex organization while maintaining the ability to be decisive and forthright in a consensus-driven environment;

- Strengths as a team leader in hiring, developing and managing a high-producing team of privacy experts;

- Excellent project management skills to effectively manage multiple ongoing projects and coordinate activities between the University and Hospitals. Demonstrated ability to effectively prioritize work and meet deadlines in a fast-paced environment;
• Superb interpersonal communication and presentation skills to clearly articulate developments in privacy laws, regulations, and compliance across the organization;

• Driven by metrics and outcomes with success implementing evidence-based changes;

• The ability to passionately model and demonstrate consistently high standards of professional ethics, integrity, and trust embodied in the values, philosophy, mission, and vision of Stanford University;

• Experience with academic research and HIPAA strongly preferred; Knowledge of FERPA a plus;

• Presence in national privacy organizations a plus;

• A bachelor’s degree is required. JD or master’s degree in business or related field preferred. Certification in Information Privacy Professional is ideal, but not required.
About Odgers Berndtson

Our reputation at the top of the executive search profession is over 50 years old. With offices in over 60 cities worldwide, our experienced executive search specialists operate with absolute discretion, integrity and care, and are expert in finding exceptional individuals for challenging roles.

Contact Information

Please submit a comprehensive resume and cover letter which sets out your interest in the role and shares the aspects of your experience relevant to the required criteria. The preferred method of application is by email at: Stanford.CPO@odgersberndtson.com

Kathryn Ullrich
Partner, Technology
O: +1 650-567-5035
M: +1 415-902-6756
kathryn.ullrich@odgersberndtson.com

Monica Burton
Partner, Education
O: +1 646-461-7723
M: +1 917-825-2961
monica.burton@odgersberndtson.com