VERSION 3.0

January 26, 2023

DREXEL UNIVERSITY
Office of
Compliance, Policy and Privacy Services

DREXEL UNIVERSITY
PRIVACY PROGRAM PLAN

PRESENTED BY: KIM GUNTER
VICE PRESIDENT AND UNIVERSITY CHIEF COMPLIANCE AND PRIVACY OFFICER

CONTENTS

INTRODUCTION

As stated in the Strategic Plan, Drexel University ("Drexel," or "University") is an urban research university that integrates education, scholarship, diverse partnerships, and our global community to address society's most pressing challenges through an inclusive learning environment, immersive experiential learning, external partnerships, transdisciplinary and applied research, and creative activity. We prepare graduates of diverse backgrounds to become purpose-driven professionals and agents for positive change.

Drexel University values the privacy of personal information and personally identifiable information (PII), including any information that could potentially be used to identify a particular person. PII includes personal information such as an individual's full name, home or residential address, email address, telephone number and date of birth. PII also includes sensitive information such as an individual's social security number, passport number, driver's license number, and certain financial information. There are many laws that protect PII such as laws related to health information, often referred to as protected health information (PHI), and student education records, including non-directory information.[1]

In compliance with federal, state and international privacy and data protection laws, rules and regulations, Drexel University is committed to protecting the privacy and confidentiality of the personal information entrusted to us by Drexel students, faculty and professional staff, as well as research participants and patients, and others. In coordination with our Strategic Plan and Code of Conduct, this Drexel University Privacy Plan ("Privacy Plan," or "Plan") articulates and defines frameworks, requirements, standards and guidelines of information privacy and data protection that are designed to support and enhance the University's protection of personal information. The Privacy Plan further details the operational structure of the Drexel University Privacy Program and offices that, working in conjunction with schools, colleges, departments and business units of the University, are responsible for the management and oversight of the University's information privacy and data protection efforts.

PRIVACY AND DATA PROTECTION FRAMEWORK

The Drexel University Privacy Program ("Privacy Program," or "Program") is designed in reliance upon the Fair Information Practice Principles (FIPPs) as first articulated in a 1973 report of the U.S. Department of Health, Education and Welfare.[2] FIPPs are widely accepted in the U.S. and internationally as a general framework for analyzing privacy risk and determining appropriate

---

1. Hereinafter, the terms "personal information," and "personally identifiable information," and "PII" will be used interchangeably and will include but not be limited to health, student and other personal information processed at Drexel University in the furtherance of its teaching, research, and healthcare mission.

2. U.S. Department of Health, Education and Welfare, *Records Computers and the Rights of Citizens, Report of the Secretary's Advisory Committee on Automated Personal Data Systems*, DHEW Publication No. (OS)73-94, July 1973, available at http://aspe.hhs.gov/reports/records-computers-rights-citizens. As stated therein, the fundamental "safeguards requirements" for personal privacy in automated systems include:

- There must be not personal-data recod-keeping systems whose very existence is secret.
- There must be a way for an individual, to find out what information about him is in a record and how it is used.
- There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.
- There must be a way for an individual to correct or amend a record if identifiable information about him.
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.

mitigation strategies.[3] As such, to ensure that Drexel University maintains an effective privacy program, the Program has three primary goals:

1. To promote a culture that requires the protection and confidentiality of personal information and respects the individual's right to exercise control over personal information,
2. To establish principles for the Drexel community regarding the accountable, sensible and transparent processing[4] of personal information, and
3. To provide the basis for confidence and trust in processing of personal information in University activities, programs and systems.

To operationalize these goals, the Drexel University Privacy Program is built upon the framework of the recognized FIPPs,[5] including each of the following elements:

1. **Transparency:** The institution should be transparent and notify individuals regarding collection, use, dissemination, and maintenance of Personally Identifiable Information (PII).
2. **Individual Participation:** The institution should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. The institution should also provide mechanisms for appropriate access, correction, and redress regarding use of PII.
3. **Purpose Specification:** The institution should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose(s) for which the PII is intended to be used.
4. **Collection Limitation and Data Minimization:** The institution should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).
5. **Use Limitation:** The institution should use PII solely for the purpose(s) specified in the notice. Sharing PII should be for a purpose compatible with the purpose for which the PII was collected.
6. **Data Quality and Data Integrity:** The institution should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.
7. **Security:** The institution should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

---

3. National Institute of Standards and Technology, U.S. Department of Commerce, *Glossary, Fair Information Practice Principles*.
4. In this Privacy Plan, the term "processing" shall mean any operation or activity, or set or operations or activities, performed on personal information during the data lifecycle from creation or collection of that information to destruction or disposal of information. Processing shall include access, creation, collection, recording, organization, structuring, storage, maintenance, adaptation or alteration, retrieval, consultation, use, disclosure (including disclosure by transmission), dissemination or otherwise making available, alignment or combination, deidentification, restriction, erasure or destruction or disposal of personal information.
5. The Fair Information Privacy Practice Principles (FIPPs), U.S. Department of Housing and Urban Development, hud.gov/program_offices/officeofadministration/privacy_act/documents/privprin, last accessed February 16, 2022.

8. **Accountability and Auditing:** The institution should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

In support of FIPPs, the Drexel University Privacy Program defines the scope of conduct in the processing of personal information expected of University community members in pursuit of the University's strategic goals.

THE DREXEL UNIVERSITY PRIVACY PROGRAM

Drexel University recognizes that compliance with the complex and rapidly changing privacy and data protection laws and regulations that affect the University's processing of personal information is often difficult. The Privacy Program is designed to help guide compliance with these standards.

Office of Compliance, Policy and Privacy Services

The Privacy Program is housed in the Office of Compliance, Policy and Privacy Services, whose mission is to help members of the Drexel community live out the core values established by the University's Code of Conduct. As a department within the Office, Privacy Program Services (PPS) oversees the Privacy Program for the University by supporting the legal, business, professional and ethical vision, principles and standards that guide us today and move us into the future. PPS works together with faculty, professional staff and students to ensure Drexel practices and systems protect the privacy and confidentiality of personal information, and to further adherence to applicable privacy and data protection laws, regulations and other standards in support of the longstanding academic, research and healthcare missions of Drexel University.

Everyone in the Drexel community is responsible to work to satisfy the teaching, research and healthcare delivery missions of the University. Thus, the Privacy Program implements the FIPPs to assist the University community in protecting the privacy and confidentiality of personal information entrusted to us.

TRANSPARENCY

Drexel University is committed to ensure individuals who share their personal information with us are informed about our practices with respect to their PII. Drexel is not in the practice of secretly collecting personal information. The University will provide individuals clear and accessible notice, often in the form of privacy statements, regarding the processing of their information including but not limited to how information is created, collected, used, maintained, disseminated, and disclosed.

Generally, the University collects personal information to provide educational, teaching, research, healthcare, and local and global community service and engagement activities. To perform and provide these services and activities, it is often necessary to collect, maintain, use and disclose personal information. Drexel University is committed to transparency in the processing of personal information of its students, faculty, professional staff, research participants, patients and others.

INDIVIDUAL PARTICIPATION

At Drexel, students, faculty, professional staff and others have the right to participate in the processing of their PII. We expect Drexel community members to participate in Drexel's processing of their PII by reading and acting upon agreements, statements, notices and policies provided to the individuals regarding their information.

We encourage individuals to exercise their rights related to Drexel's use and disclosure of their PII through mechanisms that afford the individual the ability to exercise appropriate choice regarding the disclosure of their PII; consent, as required, to the processing certain types of PII; request amendment of inaccurate information; and complain regarding the use and disclosure of their PII. Individuals may also request access to the personal information the University holds about them. However, sometimes, we may not be able to provide the individual with access to all their personal information and, where this is the case, we will tell the individual why.

Complaints and Incidents

Individuals who believe their PII has been misused or inappropriately disclosed, or who wish to make a complaint about the way we handle their personal information, may contact the Chief Privacy Officer or PPS at privacy@drexel.edu. Individuals may also contact PPS directly to ask questions or discuss and report any suspected privacy incidents and unauthorized uses or disclosures of PII. We will acknowledge all received complaints, inquiries or reports and respond to the reporter regarding the complaint, inquiry or report within a reasonable period of time.

Drexel Compliance Hotline

While we make every effort to protect the privacy and confidentiality of the personal information we process, there may be times when individuals believe or suspect an improper use or disclosure of PII that may indicate fraud, violations of law or regulation, or non-compliance with the University's Code of Conduct, or any other Official University Policies or procedures. In accordance with Drexel's Reporting Allegations Policy, Drexel community members who have a reasonable basis for suspecting improper use or disclosure of PII that may indicate fraud, violations of law or regulation, or non-compliance with our Code of Conduct and Official University Policy should promptly notify their supervisor or manager, the Chief Privacy Officer or designated PPS representative, or contact the Drexel Compliance Hotline.

The Drexel Compliance Hotline is an easy-to-use, confidential reporting hotline hosted by an external, third-party provider, EthicsPoint. The Drexel Compliance Hotline is accessible 24 hours per day, 365 days per year, by phone or via the online, web-based reporting mechanism. Reports to the Drexel Compliance Hotline will be investigated promptly and fairly. Members of the Drexel community may report to the hotline anonymously. Individual community members who report suspected improper conduct to the Drexel Compliance Hotline, in good faith, will not be subject to retaliation or harassment.

PURPOSE SPECIFICATION

Drexel University communicates the legal and regulatory authority that permits its collection of PII from students, faculty, professional staff and others prior to such collection. By providing individuals with notice of the specific purpose for which their PII is collected and the legal or regulatory authority that permits such collection, Drexel conveys its commitment to comply with those standards. Accordingly, Drexel is committed to use, store, maintain, and disclose PII only for the purposes specified. When the need to process PII changes from the purposes specified, Drexel's privacy compliance process requires that individuals are promptly notified, and where necessary, appropriate individual consent is obtained, prior to processing PII for any new, changed, or additional purposes.

COLLECTION LIMITATION AND DATA MINIMIZATION

Drexel University understands that when individuals share their personal information with us they are trusting us to protect the privacy and confidentiality of that information. Individuals also trust that the information collected will be limited to the minimum amount of information needed to achieve the stated purpose for which the information is collected. This relationship of trust extends to all Drexel community members and those acting on behalf of the University in the use and disclosure of PII. Drexel students, faulty, professional staff and others acting on behalf of Drexel are responsible to work with the Chief Privacy Officer and the PPS team prior to the collection of PII to minimize the collection of PII and to ensure the collection of PII in accordance with applicable law, rules, regulations, policies, the Drexel Code of Conduct and other standards and principles for data protection and handling.

Drexel privacy compliance processes require Drexel members to only collect PII that is directly relevant and necessary to accomplish the specified purpose for which the information is being collected. When PII is collected and processed, it must be retained only as long as is necessary to fulfill the specified purpose, in compliance with the Records Management Policy.

USE LIMITATION

Drexel University limits its uses of PII to those that are permissible under laws, rules and regulations applicable to its mission and as appropriately articulated in notices to individuals. At times, Drexel's uses of PII may include the sharing and disclosure of PII within the Drexel community and to business partners, vendors, agents and others.

Training and Education

In the Drexel community, use of PII is limited to personnel who have an authorized need-to-know the information in the furtherance of their responsibilities at Drexel. Privacy and data protection training and education provide University community members with the information necessary to understand the law, regulations, rules, policies, and our Code of Conduct to ensure the protection of the information processed. Regular and specific privacy and data protection training and education are important to the job requirements of Drexel University employees and may be required upon hire and as specified for certain job classifications. Training is administered through the Drexel University Enterprise Learning program and tracked in the employee's record. Drexel Privacy Program Services offers ongoing training and education specific to important privacy and data protection-related issues, employee job duties, and current events through the creation and delivery of web-based and live courses, as well as one-on-one discussions working in collaboration with relevant colleges, schools and departments.

As a vibrant institution of higher education, Drexel University shares PII with external business partners, vendors, agents, and others when such sharing or disclosure is compatible with the University's mission, the original purpose for the collection of the personal information or as required by law or pursuant to an authorized written information sharing agreement.

Data Agreements Matrix

Each member of the University community has a responsibility to conduct themselves ethically and in compliance with the law. At times, community members are asked to enter into agreements related to the processing of personal information entrusted to Drexel. To help community members appropriately respond to these requests and ensure that only authorized Drexel leaders execute the associated agreements, the Data Agreements Matrix is a resource provided to help Drexel

community members learn, understand and locate the appropriate individual to contact with questions or concerns about key data agreements and associated compliance. The Data Agreements Matrix communicates the University mission of shared accountability for privacy and data protection and furthers the University's culture of privacy, confidentiality, collaboration, openness, honesty and integrity.

The information contained in the Drexel University Data Agreements Matrix is provided for general guidance and is not intended for or in the place of legal advice. While effort is made to keep information up-to-date, delays or omissions may occur due to the ever-changing nature of University programs and resources to better serve the community, and the nature of change associated with the included laws, rules, regulations and University resources.

DATA QUALITY AND DATA INTEGRITY

When collecting personal information, Drexel University strives to collect information directly from the individual who is the subject of the information as much as it is practicable to do so. This helps to ensure the quality of the information, its accuracy, timeliness, completeness and relevance for the purpose it is collected. When it is not practicable to obtain information from the individual, then we will use only reputable sources to collect PII. When the information in Drexel systems contains errors, individual information subjects may request amendment of their information.

SECURITY

Drexel University has established reasonable administrative, technical, and physical safeguards to protect PII in proportion with the foreseeable risk and degree of harm that would result from the unauthorized access, use, modification, loss, destruction, dissemination, or disclosure of personal information.

Since the privacy and data protection functions at Drexel uniquely rely upon the University's information security policies, protocols and practices, the Privacy Program works closely with Drexel Information Security and the Chief Information Security Officer to ensure that reasonable administrative, technical and physical security controls are appropriate to protect the level of sensitivity of the information maintained. The FIPPs are incorporated into the implementation, execution, review and decommissioning of Drexel information systems and processes by employing the Privacy by Design framework and principles into the development and operation of information systems, networked infrastructure, and business practices that process personal information.

ACCOUNTABILITY AND AUDITING

Chief Privacy Officer

As an institution of higher education, Drexel University processes PII as we have authority to do so, as identified in the appropriate notice or privacy statements provided to individuals. Oversight of this function is under the direction of the Vice President and University Chief Privacy Officer (CPO), who reports directly to the Executive Vice President, Treasurer and Chief Operating Officer. The CPO has reporting obligations to the President and Audit Committee of the Board of Trustees. In this role, the CPO manages the day-to-day coordination of privacy and data protection efforts throughout the University, thereby helping to ensure that the University fulfills the obligations of its mission and maintains the necessary safeguards to support its operations and regulated activities.

The CPO is responsible to oversee and manage Drexel University Privacy Program professional staff by ensuring that professional staff are equally tasked with staying current on privacy and data protection standards, issues and trends. Privacy Program professional staff are required to obtain and maintain recognized industry certifications, regularly attend training and education seminars and conferences, read relevant articles and publications, and participate in professional networking.

Drexel community members who are responsible for the purchase, implementation, or ownership of programs, systems and applications that process PII are responsible to ensure initial, regular and periodic review of systems by Drexel Information Security and the Privacy Program Services to ensure that uses of PII are consistent with the purposes articulated for the collection of that information.

Privacy and Security Committee

Drexel University established a Privacy and Security Committee within the senior management and key units of the University to ensure that all laws, regulations and policies affecting the University and its activities are obeyed. The Privacy and Security Committee is responsible for advising the University Chief Privacy Officer in the oversight and maintenance of Privacy Program initiatives and activities.

The Privacy and Security Committee regularly reports to the Audit Committee of the Board of Trustees through the University Chief Privacy Officer. Members of the Privacy and Security Committee include, at a minimum, the Chief Privacy Officer and Chief Information Security Officer as co-chairs of the Committee. Other Committee members include multidisciplinary professional staff from privacy, information security, information technology, data warehouse, research, healthcare, and risk management functions within the University. A representative from the Office of the General Counsel also serves as an advisor to the Committee.

As appropriate, and upon advice of legal counsel, the Committee may commission audits of Drexel systems and files. Audit of personal information in Drexel systems and applications is an essential function of the University's Privacy Program for effective compliance with applicable legal and regulatory standards. As part of Privacy Program processes, system audits are conducted to ensure personal information is accurate, relevant, timely and complete. Privacy Program audit activities ensure information is "scrubbed" and corrected or disposed as appropriate in compliance with the Records Management Policy. The privacy audit function oversees periodic assessment of key privacy risk areas, providing review, coaching and training to University staff, recommending disciplinary action when improper actions and activities related to personal information are identified.

Approved: March 8, 2022 by the Audit Committee of the Drexel University Board of Trustees
Updated: January 26, 2023