University Counseling and Psychological Services
Lehigh University
Data Policy Statement
February 10, 2012
Updated August 27, 2018

1. Policy Constituents: Lehigh University Counseling and Psychological Services (UCPS) policies and procedures addressing the acquisition, utilization, and distribution of data acquired by UCPS staff, account for and are related to the following constituents: undergraduate students, graduate students and alumni who currently use or have used UCPS direct services (i.e. crisis assistance, group, individual, couples or family counseling/consultation); current and former graduate students who applied for or served in practicum and graduate assistantship positions; current and former work-study students; and current and former UCPS employees and employment applicants.

2. Constituents: Service constituents (i.e. "clients") who currently use or have used UCPS direct services are asked to share the following demographic data: name, SSN (or Student ID), e-mail address, phone number, birth date, race/ethnic origin, academic class, major, college affiliation, referral source, history of previous psychological treatment, current psychiatric medication(s), presenting concerns, and history of suicidal ideation or attempt. Also in the file is research data related to exercise, sleep, information on flourishing, and other "wellness" related information. Other data collected by UCPS staff and stored on the computer database includes: number and types of contacts, problem diagnosis, level of symptom severity/global assessment of functioning, consultation and session notes, intake and termination reports/summaries, psychological assessment raw data and reports, and relevant email and other communications.

   Employee and work participant constituents are expected to share demographic data, birth date, SSN, employment resume/vita, LU work evaluations, and necessary salary information within the frame of EEOC guidelines.

3. Confidentiality: Security and privacy of constituent data is safeguarded via UCPS policy and practices designed to meet the Health Insurance Portability and Accountability Act (HIPAA), American Psychological Association (APA) and State of Pennsylvania Guidelines. These guidelines specify that *Protected Health Information* (PHI) shall not be shared without written client authorization. UCPS staff also follows APA Ethical Guidelines (APA, 2017) regarding client privacy and confidentiality and carefully safeguard all client information with the exception of circumstances in which an individual is assessed to be of imminent danger to him or herself or others, cases of suspected child abuse, court-ordered requests and worker's compensation claims. Clients are informed of the limits of confidentiality at the time of their first face-to-face contact and provided with a web based copy of the HIPAA guidelines and a written copy if requested. Clients are informed that their UCPS records containing PHI are protected and confidential, and each client signs a form acknowledging understanding of this, with this acknowledgement kept in the client's chart. The privacy policy is

available in the UCPS and on our website for review at all times. In cases such as a university mandated Health Review where a committee comprised of the Dean of Students, the Health Center Director, and the UCPS Director evaluate and share information on a student, and in all other situations where information about a student is shared within the university, FERPA rules will apply in addition to those acknowledged in the preceding statement.

UCPS employee information such as salary and employment evaluations is protected by standard professional norms governed by “need to know” status and EEOC guidelines and by the “employee” being made aware of its utilization or distribution if information is shared specific to the individual.

4. Access to Data: UCPS does not permit access to or distribution/publication of any individual data outside the UCPS without the consent or awareness of the individual (as noted in #3 above). Within the UCPS, client data is accessible by all professional staff and by other staff on a “need to know” basis determined by standard supervisory relationships. All data regarding UCPS clients or “employees” are shared only in group aggregate and summary form and only when the aggregate data disallows identification of individual data (i.e. if there is only one Native American on campus, we would not report utilization or diagnosis related to Native American clients). Such summary data is summarized by national organizations and presented in summary form, with summary data specific to Lehigh University protected by a password code number.

5. Distribution of Data: UCPS employees discuss and distribute data in aggregate form only after consultation with and approval by the director or assistant director. Aggregate data is provided annually to three national organizations of which the director is a member and whose questionnaires he helped design, the Association of university and college counseling center directors (AUCCCD), the Maryland Mental Health Professionals of Color, and the Center for Collegiate Mental Health (CCMH) research center housed at Penn State. In regard to other external requests for data, (e.g. newspaper reporter requests or for research), it is UCPS policy to consult first with personnel in Communications and Public Affairs and with the university Institutional Review Board (IRB) and then if authorized, to discuss and release only aggregate data. Individual data is not shared unless requested by the individual and consent is formally authorized. Any use of individual data for research purposes and distributed outside the university will occur only if IRB approved.

6. Data Maintenance: Data on client constituents is maintained for seven years according to Commonwealth of PA guidelines. All other data is maintained for 10 years. Confidentiality is maintained in the disposal of records, which for paper products involves document shredding and for computer based data, is deleted from the Titanium server.

   The UCPS retention of data policy is the same for electronic and paper - - although the policy focuses on the retention of the data for the necessary length of time, rather than on the disposal or destruction of the data files at the end of the required period (since this is increasingly difficult to do when computer based).

7. Security Training: All members of the UCPS, including professional staff, non-exempt staff, graduate student employees and trainees, work study students, and student peer educators are given an orientation to the privacy and confidentiality requirements of a psychological services center. It is understood by all members of the UCPS that a breach of this standard entails severe legal and significant psychological risk to the Center's staff and clientele and would thus entail an immediate performance review with possible termination of employment.

8. Data Security: Security of the data stored physically in the UCPS is protected by staff monitored and locked cabinets. The UCPS stores all other client data in the Titanium Schedule which is counseling center management software designed specifically for university and college counseling centers and purchased from Titanium Software Inc. Titanium Schedule uses Microsoft SQL Server 2000 (or MSDE 2000) to store data and at Lehigh, the application and data is stored on a stand-alone server housed in the mechanical room of the computing center. Access to the application and data is only available through MS Terminal Services and is restricted on two levels: users in the counseling group and computers in the counseling office. This setup allows the application to access the data without the clinical users having direct access to the data files, thus preventing users from attaching the data files (e.g. an Access database) to an email and sending them off site, or copying them to a disk or CD. In addition, information transmitted between the server and desktop is encrypted, and password based access protects information at the desktop. LTS has two staff members specifically assigned to work on this data system.

   The system also has HIPAA compliant features like automatic inactivity logout, audit trails, and internal security levels to restrict access to various parts of the application. Computer based data is currently protected by passwords and Lehigh University LTS designed security systems.

University Counseling and Psychological Services
August 2018
Ian Birky, Ph.D., Director