Lehigh University
Athletics Department Data Policy Statement
Date: October 11, 2018
Policy and Procedures Regarding Security and Release of Data

We are required by FERPA (Family Educational Rights and Privacy Act), HIPAA (Health Insurance Portability and Accountability Act), and other federal regulations to protect the privacy of every person who inquires about varsity athletics participation, applies for admission, matriculates at Lehigh University or is employed by, supports monetarily or is an alumnus of the Lehigh University Athletics Department.

Access to FERPA protected records is granted after a written agreement to University and FERPA regulations has been completed and/or the LTS-provided ATH-SECURITY online training module that covers FERPA and HIPAA has been completed in Coursesite. The access to personal and financial records is granted based on the person's job description and needs to perform their roles. The access is proposed by the Dean of Athletics or his designate and approved by the Controller's Office, Registrar's Office or other appropriate campus office.

The Department of Athletics does not release information that would directly be attributed to one individual in accordance with required regulations. Public reporting is done through the Office of Institutional Research, the department's Sports Communications staff or another designated employee within the department. The data are shared only with governing bodies or internally with departments that need the information for the conduct of their duties. Data transfers that include directory, financial and academic data are made to the National Collegiate Athletic Association (NCAA), Patriot League Office (PL) and the federal government. Data loads that include directory, financial and academic data are also provided to JumpForward (Athletics Management Software), SportsWare (Sports Medicine Management Software), and to the NCAA systems through an encrypted website. All 3rd-party data management/collection systems, such as Jump Forward, SportsWare, SIDEARM Sports, Inc., Paciolin, and ActiveNetwork, are always vetted and approved by the University's Chief Information Security Officer before adoption.

The release of any additional information must be approved by the Dean of Athletics. Information about student-athletes (academic achievements, injury status, etc.) is not released publicly without the advance consent of those individuals. Sports Medicine or Sports Communications will get verbal permission, in addition to signed documents from the individual to give HIPAA compliant information to the media or for using in our departmental press releases.

Release of information about any constituencies listed above is limited to those that have legitimate educational reason or job function need to see the data. Both discussion and release of this data are limited to the discretion of full time department staff.

Data storage is maintained for a minimum of 7 years (as required by the NCAA) and financial records are maintained for a minimum of 3 years. Confidentiality is also maintained in the disposal of records. Records are shredded by staff and hired student workers. Records have also been shredded at the Bethlehem Recycling Center by appointment.

Prospective Student-Athlete:
The department collects Prospective Student-Athlete data that potentially includes: directory information, Social Security Number (financial aid process only), Date of Birth, transcript information, parent information, sports specific information, medical history (of a limited sample of PSAs), and financial information. Data are obtained through written letter or online forms completed by the prospective student-athlete and stored electronically and infrequently in hard copy. Only directory type information is required. Admissions decisions are only released by admissions staff members and athletic ratings are internal and only shared between athletics and people granted access to the Banner table noting these ratings. Financial aid information is shared by the department and the Office of Financial Aid. The access to personal and financial records is requested by the Dean of Athletics or his designate and granted by the appropriate data steward based on the person's job description and needs to perform their roles. Hard copy data on prospective student-athletes is kept for a minimum of 8 years and disposed of by shredding hard-copy information and destroying tapes or CDs. Reports are kept beyond 8 years. Electronic data is backed up on CD or the server when removed from current year files.

Student:
The department collects Student data that includes: directory information, university ID, date of birth, ethnicity, high school information, enrollment information, parent information, health information, sports specific information, financial information and vehicle information. When applicable, HIPAA and FERPA regulations are followed by all staff who have been granted access to such data based on their role. Student-athletes sign consent forms allowing release of information and also separate forms for release of academic data within the university for reporting and to the NCAA. The access to personal and financial records is requested by the Dean of Athletics or his designate and granted by the appropriate data steward based on the person's job description and needs to perform their roles. Student-athlete data are stored primarily in electronic form in databases with limited data stored in hard copy. Hard copy data on students are kept for a minimum of 7 years and disposed of by shredding hard-copy information and destroying tapes or CDs. Reports are kept beyond 7 years. Electronic data is kept backed up on CD or the server when removed from current year files.

Athletics Staff (staff and work study):
All official records for University staff (including athletics staff) are maintained in the Office of Human Resources, wherein appropriate controls of access and dissemination are monitored. The Athletics Department collects and maintains staff data that are useful for functional operations (ex. directory information, University ID, employment dates and basic personnel transactional records). Employee paperwork is all processed with the appropriate offices

(Human Resources, Financial Aid and Payroll). During their new staff orientation, Athletics staff are provided an overview on department policies. All staff (including work study students) complete an online security course provided by LTS to familiarize them with FERPA (Family Educational Records and Privacy Act) and HIPAA. Access to personal and financial records must be requested through the Dean of Athletics or his designate and is granted by the appropriate data steward based on the person's job description and needs to perform their roles. All data are maintained in spreadsheets or locked files and only basic biographical information is kept in an electronic database.

Volunteers:
The department collects Volunteer data that include: directory information, University ID, volunteer 'employment' dates and personnel records. Volunteers are given an overview on department policies and must complete an application. The Department staff are responsible for making a request for data if required for a project volunteers will be working on. Volunteer personnel data is not kept in permanent files.

Alumni:
The department uses and collects data on Alumni. Information is requested from the Development Office and all applicable University policies are followed. The access to personal and financial records is requested by the Dean of Athletics or his designate and granted by the appropriate data steward based on the person's job description and needs to perform their roles. Data are shredded when no longer needed or returned to the Development Office. The data are only requested and kept as needed.

Camp Information:
The department collects paperwork for employees and attendees of Clinics and Summer Camps. Data include: employment paperwork (i.e. I9, W4), directory information, health information and release of liability waivers. The access to personal and financial records is requested by the Dean of Athletics or his designate and granted by the appropriate data steward based on the person's job description and needs to perform their roles. The camps program uses ActiveNetwork, a 3rd party SAS system, to collect camper data (including health information and participation waivers), employee data, and payments. The data for employees of the current camp year are maintained in payroll and copies are kept in the camp office which is locked when not staffed. Any hard copies of registration forms and health forms are also kept in the camp office. Registration waivers and health data forms are disposed of after 3 years by shredding. Archived records from previous years are stored in a locked storage room in Rauch Field House next to the camp office. All electronic data is kept.

Electronic Data:
The department has one secure virtual server located in the on-campus server room that is maintained by our internal LTS staff. This server houses the SQL data and databases for historical camp data, historical prospect data, and current student and staff and competition

schedule data.This server is accessed securely through Active Directory and restricted IP and all web traffic to and from the athletic servers is SSL encrypted.

The server room also hosts a 3rd party machine that runs our football video system by XOS. This data only includes video clips of football games.

The department uses a number of electronic and/or web-based systems for daily operations. The outside vendor that is currently used for data collection in camp registration is ActiveNetwork, in merchandising (online store) it is Advanced-Online, in sports medicine it is SportsWare, in tickets it is Paciolin, and for recruiting and student-athlete information it is Jump Forward. Our athletics website, lehighsports.com, is hosted by SIDEARM Sports, Inc. All information posted to the website is done by Lehigh Administration or by SIDEARM Sports under the direction of Lehigh administrators.

For the department's Ticketing System, Paciolin is the vendor. Paciolin is also the vendor for Zoellner Arts Center. Paciolin follows the standards of the Payment Card Industry Data Security Standard (PCIDSS). We also ensure that all payment processing is done only via a validated PCI Point to Point Encryption (P2PE) method. All ticketing computers are kept in a locked ticket office.

The Department has used a web-based program from the NCAA that is designed for standardized reporting of our records as detailed previously. The files are now loaded through JumpForward or via XML feed from Banner for this standardized reporting and used in conjunction with some of the NCAA systems.

The Department uses JumpForward as the Recruitment Database and for some Student-Athlete data management. Much data is transmitted through an api or secure requested file load. Staff access to the recruitment system is controlled via SSO login controls tied to the university's Active Directory system. Roles and permissions are defined within Jump Forward for tighter control over features and functionality. This system has been approved by Lehigh's Chief Information Security Officer as having met all of Lehigh's data security standards. Documentation of Jump Forward's data security policies and standards are available on the Athletics Google Drive.