JOHNS HOPKINS UNIVERSITY

POLICE DEPARTMENT

RECORDS MANAGEMENT

ADMINISTRATIVE PROCEDURE #210

Responsible Executive:
Chief of Police

Responsible Office:
Vice President for Public Safety

Approved by:
Dr. Branville G. Bard Jr.

Issued: 07/25/2024
Revised: N/A

Table of Contents

Policy Statement

The Johns Hopkins Police Department (JHPD) records management program was established to organize, maintain, and effectively manage access to physical and electronic records created by the JHPD. The organization, retention, and appropriate disposal of records no longer legally or institutionally required will be administered according to applicable laws, Johns Hopkins policy, and this Directive.

In addition, this Directive sets the standards and criteria for the public release of video recordings that capture critical incidents involving JHPD officers. This Directive is intended to balance two important interests: the public's interest in transparency and police accountability, and the privacy interests of the individuals depicted in such videos. The public has a strong interest in obtaining timely access to information, including video footage, regarding incidents where officers use lethal force or where a person has died or suffered a serious injury as a result of a police encounter or while in police custody. At the same time, the individuals who appear in these videos have a privacy interest that must be considered. These individuals include not only the involved individuals and the police officers but also witnesses, bystanders, and the persons

upon whom force is used. There are considerations, such as preserving the integrity of related investigations, that may justify a delay or deviation from the standard procedure, and these considerations are also detailed in this Directive.

This Directive also outlines the process and procedures for public requests of JHPD records; service of civil complaints, subpoenas, and other legal process related to JHPD members and incidents; the sharing of JHPD information with Johns Hopkins; and student and patient privacy protections.

Who Is Governed by This Policy

All personnel, including sworn, nonsworn, and contractual or voluntary persons in service with the JHPD, are governed by this Directive.

Purpose

This Directive provides a framework for the JHPD to organize, maintain, and effectively manage access to physical and electronic records created by the JHPD and to meet the JHPD's obligation to comply with federal, state, and other legal requirements for records retention and destruction, as well as Johns Hopkins's record retention and destruction schedule. In addition, this Directive outlines the JHPD's release of critical incident records; responses to public requests for JHPD records; service of civil complaints, subpoenas, and other legal process; dissemination of records within the JHPD and Johns Hopkins; and privacy protections related to student and patient records.

Definitions

Civil Complaint:	A legal document that initiates a lawsuit and informs the person being sued of the claims against them. Typically, the person or entity that initiates the lawsuit is called the plaintiff and the person or entity that the lawsuit is against is called the defendant.
Critical Incident:	For purposes of this Directive, a critical incident includes any event in which a member uses force that results in hospitalization or death, discharges a firearm, strikes a person in the head with an impact weapon, or engages in a vehicle pursuit. In addition, it includes any in-custody serious injury or death, as well as the serious injury or death of a member while performing their JHPD duties. Critical incidents may also include situations in which a person who is suspected of a violent crime that poses an imminent danger to the public escapes or flees or there is an active assailant, hostage, or barricade incident on campus. Finally, critical incidents can include any other incident or complaint of misconduct that the JHPD Chief of Police designates as a critical incident.
Directory Information:	Pursuant to the Family Educational Rights and Privacy Act (FERPA), information contained in an education record of a student that it would not generally be considered harmful or an invasion of privacy to disclose. FERPA permits institutions to establish and disclose without consent a student's directory information provided

	that it has given public notice to students in attendance regarding (1) the specific types of personally identifiable information that it has designated as directory information, and (2) the rights of students to refuse disclosure of their directory information. Johns Hopkins has established the following as directory information: • Name of a student who is in attendance or who has been in attendance, • Name pronunciation, • Local address of a present or former student, • Johns Hopkins email address of a present or former student, • Local telephone number of a present or former student, • Major field of study of a present or former student, • Participation in Johns Hopkins Athletics (limited to hometown, sport, height, and weight), • Dates of attendance, • Degrees and awards received, and pertinent dates, • Honors, • Photograph (still, video, audio), and • Classification (enrollment status) and level of study.
Education Records:	As defined by FERPA, education records are records that (1) are directly related to a student who is or has been in attendance at an educational agency or institution and (2) are maintained by an educational agency or institution or by a party acting for the educational agency or institution. This encompasses information or data recorded in any medium, including but not limited to handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche. Examples of education records include transcripts; class schedules; course work such as papers, exams, grades, and evaluations; disciplinary records; internship program records; and student financial records. Records relating to an individual in attendance who is employed as a result of their status as a student are also considered education records under the terms of FERPA. Education records are **not**: • Records that are kept in the sole possession of the maker, are used only as a personal memory aid, and are not accessible or revealed to any other person except a temporary substitute for the maker of the record, • Records of the law enforcement unit of an educational agency or institution, • Records relating to an individual who is employed by an educational agency or institution that are made and maintained in the normal course of business, relate exclusively to the individual in that individual's capacity as an employee, and are not available for use for any other purpose,

	• Records made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in their professional capacity or assisting in a paraprofessional capacity that are made, maintained, or used only in connection with treatment of the student and disclosed only to individuals providing the treatment (although the student may have those records reviewed by a physician or other appropriate professional of the student's choice), • Records created or received by an educational agency or institution after an individual is no longer a student in attendance and that are not directly related to the individual's attendance as a student, • Grades on peer-graded papers before they are collected and recorded by an instructor, or • Law enforcement unit records.
Health and Safety Emergency:	Situation in which appropriate parties need information to protect the student or others. Examples might include but are not limited to welfare checks, suicidal statements, concerning behaviors, etc. (20 USC § 1232g(b)(1)(I); 34 CFR §§ 99.31(a)(10), 99.36) In making a determination during a health and safety emergency, the totality of the circumstances pertaining to a threat to the health or safety of a student or other individuals must be considered to determine if there is a rational basis to support an articulable and significant threat to the health or safety of a student or other individuals. If so, Johns Hopkins may disclose information from education records to any person whose knowledge of the information is necessary to protect the health or safety of the student or other individuals. (34 CFR § 99.36)
Independent Investigative Division (IID)–Qualifying Incident:	All police-involved incidents that result in the death of a person or injuries that are likely to result in the death of a person occurring in the state of Maryland.
Individually Identifiable Health Information:	Pursuant to the Health Insurance Portability and Accountability Act (HIPAA) of 1996, individually identifiable health information is information, including demographic data, that relates to: • The individual's past, present, or future physical or mental health or condition, • The provision of health care to the individual, or • The past, present, or future payment for the provision of health care to the individual, • And that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

Law Enforcement Unit Records:	Records created by the JHPD or another law enforcement unit at the educational agency or institution, created for a law enforcement purpose, and maintained by the law enforcement unit that are not education records subject to the privacy protections of FERPA or protected health information (PHI) subject to the privacy protections of HIPAA. Law enforcement unit records are "records" as defined in this Directive.
Member:	All members of the JHPD, including employees, officers, and volunteers, unless the term is otherwise qualified (e.g., member of the public, member of the Baltimore Police Department (BPD), etc.).
National Incident-Based Reporting System (NIBRS):	NIBRS is the national standard for law enforcement crime data reporting in the United States. NIBRS captures detailed data about the characteristics of criminal incidents, including a broad array of offenses; types and amount of property lost; demographic information about victims, offenders, and persons arrested; and what type of weapon, if any, was used in the incident.
Officer:	All sworn police officers, at any rank, as defined by MD Code, Public Safety, §3-201, in service with the JHPD.
Person in Interest:	A person who is the subject of the record or, if the person has a legal disability, the parent, guardian, or other legal representative of the person.
Privacy Block:	A student may restrict the release of directory information by submitting a Request to Prevent Disclosure of Directory Information Form. If a student restricts the release of directory information, a notation appears in the Student Information System (SIS).
Process Server:	Notifies the person that a legal proceeding has been initiated against them by delivering documents such as subpoenas, summonses, and complaints.
Protected Health Information (PHI):	All individually identifiable health information held or transmitted by a covered entity, including any health care provider (such as the John Hopkins Health System (JHHS)) or its business associate, in any form or media, whether electronic, paper, or oral.
Record:	Any documentary material in any form created or received by the JHPD.
Recording:	Audio and/or video recording of an incident.
Service of Process:	The way the person against whom a complaint is filed, often called the defendant, receives legal documents and notice about a court case. The defendant must be served before the court will hear the case.
Subpoena:	A written command by the court ordering the named party to appear in court or to produce documents.
Summons:	A written notice, usually accompanied by a civil complaint, notifying a person and the court that the civil complaint has been served on all relevant parties and listing the date of the first scheduled court appearance.

Policy

It is the policy of the JHPD to properly organize, maintain, and effectively manage access to physical and electronic records created by the JHPD and to meet its obligation to comply with federal, state, and other legal requirements for records retention and destruction, as well as Johns Hopkins' record retention and destruction schedule. In addition, the JHPD will release critical incident recordings and respond to public requests for JHPD records and legal process, in accordance with all applicable legal requirements.

Core Principles

I. **Transparency:** To promote transparency, it is the policy of the JHPD to release audio and video recordings of critical incidents involving the JHPD as long as such disclosure does not jeopardize any ongoing law enforcement investigation. In addition, the JHPD shall respond to public requests for JHPD records, in accordance with the standards set forth in the Community Safety and Strengthening Act. All releases shall be made in accordance with federal, state, and local law.

Procedures

I. **General** (Commission on Accreditation for Law Enforcement Agencies (CALEA) 82.1.2, 82.1.3, 82.1.4, 82.3.6, 91.1.3)

A. Duties and responsibilities of the Records Management function include but are not limited to:

- Managing and controlling access to the JHPD's criminal, civil, and administrative records,
- Maintaining distinctive designations, security, separation of, and access to records related to adult and youth arrests,
- Collecting and reporting crime-related information consistent with the Federal Bureau of Investigation's (FBI's) NIBRS,
- Consistent with the Clery Act, 20 USC § 1092 (f):
  - Ensuring the agency's Crime Log is compiled and published,
  - Compiling and reporting required crime, referral, and arrest information to the U.S. Department of Education, and
  - Retaining related records in accordance with Johns Hopkins' retention schedule.
- Expunging and disposing of arrest records as required by law and the courts,

- Retaining and disposing of records under control of the Central Records function consistent with Johns Hopkins' records retention and destruction schedule, and
- Disseminating records information to authorized persons and entities.

B. The Captain of Support Services is the official custodian of the JHPD's records once they are uploaded or entered into the JHPD's Records Management System (RMS). These responsibilities include safeguarding official files and ensuring records are released consistent with applicable administrative and statutory requirements and following the JHU Retention Schedule Policy, Records Retention and Destruction (GOV029).

II. Records Management System (RMS) (CALEA 82.1.1.a, 82.1.1.b, 82.1.6, 81.3.3, 82.3.4, 82.3.5)

A. The JHPD's RMS contains computer-aided dispatch, report writing, and other modules used to generate, approve, track, retain, and analyze information critical to the JHPD's mission.

B. The RMS is:

- Hosted and backed up within Johns Hopkins' secure server system,
- Access controlled based on each member's individual access needs as determined by commanders, authorized by the Chief of Police, and set by the JHPD's internal system administrator,
- Password protected by a system that requires passwords be periodically changed and conform to certain standards, and
- Always accessible to authorized users from within JH's network.
- Certain operational-related records are stored or maintained outside the RMS.

III. Field Reporting System

A. The JHPD's field reporting system is primarily contained in the case management module of the online RMS. A hard-copy version of the field reporting system is in place for use only when the online system is unavailable or when otherwise directed by a commander. (CALEA 82.1.5, 82.2.1, 82.2.2, 82.2.3, 82.3.1, 82.3.2)

B. Capabilities and contents of the case management system include but are not limited to:

- Record of every incident of:
  - Public complaints and crime reports,

- Incidents that resulted in members being dispatched or assigned,
- Criminal and noncriminal cases initiated by members, and
- Arrests, citations, or summonses being issued.

- Unique case numbers assigned to every case,
- Instructions on when and how case reports must be written,
- Computer applications and forms to be used in field reporting,
- Information required in field reports,
- Procedures for submitting, processing, training, supervisory review, and approval of field reports, and
- Indexed information that includes but is not limited to:
  - All persons identified in reports,
  - Case numbers,
  - Incident types,
  - Incident locations,
  - Stolen, found, recovered, and evidentiary property, and
  - Accounting for the status of all case numbers, reports, case assignments, follow-ups, and dispositions.

C. Other forms and reports required by other JHPD bureaus and sections will be used as required by those JHPD entities. These other forms and reports include but are not limited to:

- Accident Investigation,
- Missing Persons,
- Animal Complaints & Bites,
- Maryland Uniform Complaint and Citations, consistent with the Law Enforcement Manual and JHPD Directive #442, Traffic Control & Enforcement, and
- Various charging and referral documents consistent with JHPD Directive #424, Arrests & Alternatives to Arrest, and JHPD Directive #426, Interactions With Youth.

IV. Access to Records (CALEA 82.1.1.a, b)

Members assigned records management responsibilities will ensure the following:

A. Office space used to secure physical criminal history and other operational records is designated a restricted access area.

B. Doors shall remain closed and locked except when authorized persons are accessing the records.

C. Members with access privileges are responsible for controlling and authorizing access to the office.

D. Other members are permitted to be in the records office only in the furtherance of agency business or activities that can only be conducted in the office and when they are admitted and escorted by members with access privileges.

V. Records Dissemination (CALEA 82.1.1.a, b, c, 82.2.4)

A. Members of the JHPD who need documents kept in Records Management that are not otherwise available for printing from the RMS must request these records from the Captain of Support Services by email at least two business days in advance. The Captain of Support Services will ensure:

- Records requests are promptly processed,
- Requesting members are promptly contacted if the records cannot be located or requests cannot be fulfilled,
- Printed copies of the emails or JHPD records requests are retained in case files as dissemination records, and
- The records commander is consulted when requests are not received within the required time limit.

B. Records Management members are responsible for the routine and timely distribution of various printed or electronic report copies within the JHPD, to appropriate Johns Hopkins officials, and to various officials and criminal justice agencies outside the university.

C. The handling of requests from the public will be completed in accordance with MD Code, Education, § 24-1210, and Section IX of this Directive.

VI. Criminal History (CALEA 82.1.1.c, 82.1.7, 82.3.6)

A. Records Management will maintain online and hard-copy records of each arrest. Records Management members will ensure that:

- Hard-copy arrest folders are made and arrest numbers are assigned for each person arrested.
- The MD Criminal Justice Information System (CJIS) assigns a State Identification Number (SID) to each person whose arrest is reported to CJIS. SIDs are person oriented, person specific, and linked to that person for all subsequent arrests.

B. Records Management will ensure that criminal history record information (CHRI) is secured pursuant to the FBI's CJIS Security Policy and is not released by JHPD members, except as authorized by statute and related directives. JHPD Records Management members may do the following:

- Allow people to inspect their own CHRI maintained by the JHPD.
- Allow attorneys to inspect the CHRI of their clients who were arrested by the JHPD. The right to review local CHRI does not extend to making copies of the documents.
- Allow local CHRI to be released when officers or agents from other criminal justice agencies request CHRI and delays in receiving the information from CJIS would unduly impede necessary action by requesting agencies or would violate or materially impair the substantive right of persons about whom the information is released.
    - Instances when such disclosure by Records Management members would be appropriate include but are not limited to:
        - State's Attorneys' records checks for court,
        - Court Commissioners' inquiries relating to bail hearings, and
        - Requests from another law enforcement agency during the conduct of ongoing investigations.
- Allow military recruiters to review local CHRI only after they have applied to CJIS and have been authorized to obtain locally held CHRI.
- Not allow private employers who request local CHRI to review it. Instead, they will be referred to CJIS.
- Allow investigators from certain federal agencies, without the investigators first obtaining CJIS authorizations, to review local CHRI pursuant to the Security Clearance Information Act (SCIA), 5 USC § 9101. Records Management will maintain a current list of agencies covered by the SCIA.

VII. Youth Records (CALEA 82.1.1.c, 82.1.2.a, e)

A. Records Management will ensure that hard copies of youth reports and arrest records are stored in an area that is physically separated from adult Incident Reports and arrest records within Records Management, and comply with the following guidelines:

- The storage area for youth reports and arrest records shall always stay locked unless records members are performing related work with the files.
- Arrest records of youth charged as adults are filed with adult arrestee records.
- Records members assign a distinctive, person-oriented juvenile identification number to each youth arrested. Youth are subsequently referenced by their juvenile identification number in any future arrests.

B. Hard-copy youth reports and arrest records will be removed from active youth files, stored separately when the youth reach the age of 18, and retained consistent with Johns Hopkins' records retention and destruction schedule.

C. If youth records are kept fully in the RMS, they shall be identified as confidential and access to them shall be restricted.

D. Members shall adhere to MD Code, Courts and Judicial Proceedings, § 3-8A-27, and MD Code, Education, § 7-303, for restrictions, permissions, and mandatory situations for the release or sealing of youth arrest record information.

E. Members shall adhere to MD Code, Courts and Judicial Proceedings, §§ 10-105, 10-106, for conditions relating to the expungement of youth arrest records.

VIII. Public Release of Critical Incident Recordings & Reports

The JHPD is committed to transparency and will make every effort to inform the public of critical incidents and to release critical incident recordings as soon as possible. While these procedures apply to the proactive public release of critical incident recordings involving JHPD members, they do not in any way prohibit or preclude any member of the public from making a request to view or receive JHPD records or recordings, pursuant to the procedures in Section IX.

A. The Independent Investigative Division (IID) of the Maryland Attorney General's Office investigates, and has authority to criminally prosecute, all police-involved incidents that result in the death of a person or injuries that are likely to result in the death of a person occurring in the state of Maryland (IID-qualifying incident). Considering IID's authority and responsibility, the JHPD and the Johns Hopkins Public Safety Accountability Unit (PSAU) will confer with the IID regarding all public response and public release of records and recordings related to an IID-qualifying incident, including body-worn camera (BWC) footage.

B. For non-IID-qualifying critical incidents, after consultation with BPD, PSAU will handle the public release of all recordings. In general, the release of non-IID-qualifying critical incident–related recordings will occur no more than seven days after the incident. In most instances, the public release of non-IID-qualifying critical incident recordings will occur in less than seven days. The public release will typically be made via the public posting of the non-IID-qualifying critical incident recording on Johns Hopkins' Public Safety website.

C. On the other hand, there may be a rare occasion when the non-IID-qualifying critical incident recording cannot be released within the seven-day period, including when investigators need more time to complete witness interviews, there are technical delays caused by the need to redact information that raises privacy or safety concerns, or family members must be allowed to view the recording before it is released to the public. If the release of the recording is delayed, PSAU will notify the public that there has been a delay and state the reason for the delay.

D. In addition, to the extent possible, for non-IID-qualifying critical incidents, the Public Information Officer (PIO) will make an initial statement, after consultation with the Executive Director of PSAU, which may include any or all the following information:

- The date, time, and location of the incident,
- The type of call for service that led officers to the scene.
- Information concerning injuries sustained by any persons or an officer, and whether any persons were transported to the hospital.
- If any complaint was received, status, and type of investigation (ongoing, criminal, or administrative), and
- Basic deidentified information regarding the age, race, duty assignment, tenure, and current administrative status of the officers and involved persons.

E. Upon completion of the initial public or media notifications, the PIO, in consultation with PSAU, may continue to provide periodic updates involving an ongoing community threat, investigative status updates, and outcomes.

F. Before the public release of a non-IID-qualifying critical incident recording, PSAU shall consult with BPD, in compliance with the Memorandum of Understanding (MOU) between the JHPD and BPD, dated December 2, 2022, and the Baltimore City State's Attorney's Office or any other relevant federal, state, or local law enforcement agency, if necessary.

- Any of these agencies may object to the release of a non-IID-qualifying critical incident recording, pursuant to the process below, and may request to delay release of the recording. PSAU will inform the relevant agencies of its planned release date at least 48 hours in advance and will consider written delay requests during that 48-hour interval.
- If time permits, PSAU will meet with the requesting entity to discuss the requested delay. Any request for delay must set forth with specificity in writing:
    - The length of the delay requested (not to exceed 30 calendar days from the incident date),
    - The specific items sought to be temporarily withheld, and
    - Reasons supporting the delay due to one or more of the following factors:
        - Interfering with a law enforcement proceeding,
        - Depriving someone of fair adjudication,
        - Unduly invading personal privacy,
        - Disclosing a confidential source,
        - Disclosing an investigative technique or procedure,
        - Prejudicing an investigation, or
        - Endangering a person's life or physical safety.
- The decision to approve or deny the requested delay in the release of a non-IID-qualifying critical incident recording rests with the Executive Director of PSAU. If approved, the written request to delay release itself will be released to the public within the time period that the recording would have otherwise been released. If denied, the written request to delay release will itself be released to the public upon the denial.
- Notwithstanding the number of requests for delay of the public release of the non-IID-qualifying critical incident recording, the period of delay approved by the Executive Director of PSAU will not extend beyond the 30 days from the date of the incident, unless it would substantially interfere with the investigation of the incident or would be substantially likely to create witness safety concerns. At the end of the delay period, or if no delay is approved, the non-IID-qualifying critical incident recording will be released to the public.

G. Upon conclusion of a PSAU investigation of a non-IID-qualifying critical incident, PSAU will publicly release the critical incident investigative report.

H. At the direction of the Executive Director of PSAU, non-IID-qualifying critical incident recordings may be blurred and muted and reports may be redacted prior to public release for privacy or legal confidentiality, including recordings that feature:

- Nudity,
- Sexual assault,
- Medical emergencies,
- Behavioral health crisis,
- Victim interview,
- Personal or financial information,
- Explicit or gruesome bodily injury,
- The interior of a home or treatment facility, or
- A minor and any images or information that might undermine the confidentiality of a record related to a youth, student, or patient.
    - NOTE: This section does not establish any new rights to any third party regarding the release of JHPD recordings or records.

IX. Public Requests for Records & Recordings

A. Pursuant to MD Code, Education, § 24-1210, the JHPD shall allow a person or governmental unit to access information as a person or governmental unit would be able to access a public record of a law enforcement agency, under the Public Information Act (PIA), if the information is included in records that are:

- Created solely for law enforcement purposes, or
- Related to an arrest for a criminal offense, and
- Would be subject to disclosure under the PIA if the information were in a record created by a law enforcement agency.

B. In addition, pursuant to MD Code, General Provisions, § 4-311, all records relating to an administrative or criminal investigation of misconduct by a police officer, including administrative investigatory records, a hearing record, and records relating to a disciplinary matter, except for records related to technical infractions, shall remain confidential, but are subject to public disclosure upon request. All documents related to technical violations shall remain confidential and are not subject to public disclosure.

C. Members of the public seeking to review a JHPD recording or record in which they are a person in interest may request to do so, at any time, via telephone, in person, in writing, or via the Request for Information Form linked below. A JHPD supervisor will obtain the recording or record and facilitate the review of the recording or record for the interested party.

D. Members of the public seeking to obtain JHPD records, including BWC footage or records related to misconduct, may make a request by submitting a written request for JHPD records to the JHPD PIO via the Record Request webform, located on the Johns Hopkins Public Safety (JHPS) website under Requests for Information or in writing at:

JHPS
c/o JHPD PIO
1101 E. 33rd St.
Baltimore, MD 21218

E. Upon receipt of a JHPD record request, the PIO will acknowledge the request within five business days and will respond with the records, deny the request, or provide notice that the records do not exist within 10 days, unless it will take more time, in which case the PIO will notify the requester in the acknowledgment that it will take more than 10 days, but no more than 30 days, to provide the records or deny the request. If fees are associated with this request, the PIO will provide an estimate of costs which must be collected prior to the request being fulfilled, with the acknowledgment.

F. All requests for records and recordings, regardless of the identity of the requester or form of the record (electronic, photograph, recording, audio, paper, etc.), received by the JHPD shall be immediately forwarded to the PIO, with a copy sent to the Office of the Senior Vice President and General Counsel for JHU for review.

G. Upon receipt of the record request, the PIO will log all requests and gather the corresponding records and recordings, unless the records are related to misconduct, in which case, after being logged, the request shall be immediately forwarded to the designated PSAU member to gather the corresponding records and recordings.

- The PIO or PSAU member will make a preliminary determination as to whether the records or recordings are accessible to the public, pursuant to MD Code, Education, § 24-1210, or MD Code, General Provisions, § 4-311, and if so, any redactions that should be applied under the PIA or other applicable laws.

- The PIO will then forward the records and the request to the Office of the Senior Vice President and General Counsel for JHU for legal review to ensure compliance with MD Code, Education, § 24-1210, or MD Code, General Provisions, § 4-311, the PIA, and other applicable laws.
- Upon completion of the legal review, the PIO or PSAU member shall provide the records or recordings to the requester or issue a denial letter stating the reason the request was denied.

X. Court Orders for Records & Recordings

A. The PIO shall not accept service of subpoenas or court orders for any Johns Hopkins corporate entity, JHPD personnel, and/or records or recordings without direct authorization from the Office of the Senior Vice President and General Counsel for JHU.

B. Upon receiving notice of a subpoena or court order for JHPD records or recordings, the PIO and any other JHPD member should immediately notify the Office of the Senior Vice President and General Counsel for JHU.

C. All subpoenas or court orders for JHPD records shall be directed to Johns Hopkins and shall be served on Johns Hopkins' resident agent.

D. When a subpoena or court order requiring production of JHPD records or recordings, including BWC footage, is served on Johns Hopkins, a representative of the Office of the Senior Vice President and General Counsel will immediately notify the PIO.

E. Upon notice and receipt of a copy of the subpoena or court order requiring Johns Hopkins to produce JHPD records or recordings, the PIO shall immediately gather all responsive records or recordings and prepare a Bates-numbered copy of the original record or recording file for the Office of the Senior Vice President and General Counsel of JHU.

F. The Office of the Senior Vice President and General Counsel will prepare the appropriate response to the subpoena or court order and handle the production of the records.

G. The original file shall be returned or maintained in its original form, and a duplicate copy shall be retained by the PIO.

H. Members shall direct all inquiries by an attorney (other than an Assistant State's Attorney or an Assistant U.S. Attorney) who is seeking information about a case (open or closed), documents, JHPD policies and procedures, personnel records (including disciplinary matters), or similar requests to the JHU Office of the Senior Vice President and General Counsel.

I. Subpoenas requiring JHPD members to personally appear shall not be accepted by anyone other than the member identified, unless the member has specifically authorized the Office of the Senior Vice President and General Counsel to accept it on their behalf. Members shall not produce any records or recordings pursuant to a subpoena directed at them personally, as all records and recordings of the JHPD are in the custody and control of JH, not the member personally.

XI. Release of Information Within Johns Hopkins

A. Subject to limitations of state and federal law, information concerning Johns Hopkins affiliates shall be released when necessary and appropriate, and when needed as part of their job duties, to the following:

- Vice President for Public Safety or designee, Chief of Police, and PIO,
- Office of Hopkins Internal Audits,
- Student Affairs,
- Office of Institutional Equity, Title IX coordinator,
- Provost's Office,
- Senior Vice President and General Counsel or designee, and
- Human Resources.
    - NOTE: Any criminal history information should be redacted prior to internal Johns Hopkins release.

B. Information concerning a Johns Hopkins student, faculty member, or staff member will be provided to others within Johns Hopkins upon approval by the Vice President for Public Safety or the Senior Vice President and General Counsel, as necessary.

C. **Release of Information for Clery Act Compliance:** All release of information necessary for Clery Act compliance shall be in accordance with JHPD Directive #222, Clery Act Compliance.

XII. National Incident-Based Reporting System (NIBRS)

The JHPD participates in NIBRS. Each month, compiled data is to be forwarded to the Maryland State Police (MSP), which acts as the state clearinghouse for the FBI. All information reported by the JHPD is incorporated into the annual NIBRS report and quarterly and annual reports distributed by the MSP.

XIII. Requests From Other Criminal Justice Agencies

A. Pursuant to the MOU between the JHPD and BPD, all criminal Incident Reports and traffic stop data will be provided to BPD.

B. Records will be provided to another criminal justice agency when related to criminal or regulatory investigation and with approval from the Chief of Police and review by the Office of the Senior Vice President and General Counsel for JHU.

XIV. Receipt of Lawsuits & Summonses

Legal documents such as subpoenas, summonses, and civil complaints must be served directly upon the person to whom they are addressed, unless the member has designated the JHU Office of the Senior Vice President and General Counsel to accept service on their behalf.

A. Required Action:

- JHPD members shall not accept service of process of civil complaints, summonses, or subpoenas on behalf of other members of the Johns Hopkins or the JHPD.
- JHPD members shall, respectfully and courteously, accept service of process of civil complaints, summonses, and subpoenas in which they are a named defendant or subject of the complaint, summons, or subpoena.
- JHPD members shall not evade service of civil complaints, summonses, or subpoenas or attempt to frustrate efforts for service of process.
- JHPD members shall provide process servers with information regarding the member in question's assigned shift and the name of their direct supervisor, if asked.
- JHPD members shall not disseminate another member's home address, telephone number, or other personal information.
- Members may request the JHU Office of the Senior Vice President and General Counsel to accept service on their behalf.
- If a member receives service of a civil complaint, summons, subpoena, or other court process, they shall immediately notify their Lieutenant and, if related to their employment, follow JHU Policy Employee Indemnification and Defense (GOV015) to request defense and indemnification.

B. **Lieutenant/Commander Officer:** Upon notification that a civil complaint, summons, or subpoena exists for a subordinate, the Lieutenant/Commander shall:

- Make every effort to facilitate service of process of complaints, summonses, and subpoenas of members under their supervision.
- Where feasible, coordinate with process servers to arrange a date and time for successful service of the process.
- If necessary, order subordinates to appear at a designated time and place for service of process.
- Upon receiving notice of a civil complaint against any JHPD member, obtain a copy from the member and notify the Office of the Senior Vice President and General Counsel for JHU and forward to PSAU for investigation.

C. **PSAU:** PSAU shall complete an inquiry into all civil complaints and suits against JHPD members in accordance with JHPD Directive #350, Complaints Against Police Personnel.

XV. Student Record Privacy

A. The JHPD is committed to maintaining compliance with FERPA to protect student information by following strict access and disclosure procedures.

B. JHPD members will generally access and use only the Johns Hopkins online directory to obtain information about a student, when necessary, and will not access SIS, unless there is a health and safety emergency.

- If a student has elected to place a privacy block on their account, then their information should not be available in the online directory; to access the information in the online directory that is subject to the privacy block, members must get consent from the student and have them execute a FERPA release.
- If there is a health and safety emergency, members must request approval by the Chief of Police or their designee prior to accessing SIS.
- If there is not a health and safety emergency, then a member must have a law enforcement purpose to access SIS records and must get consent, and an executed FERPA release, from the student whose records are sought. If consent cannot be obtained, the member may only access SIS via a warrant, subpoena, or court order. (20 USC §§ 1232g(b)(1)(J), (b)(2); 34 CFR § 99.31(a)(9))

- Prior to obtaining a warrant, subpoena, or court order to access SIS, the member must request approval through their chain of command to the Chief of Police, who shall consult with the Office of the Senior Vice President and General Counsel for JHU.
- If approved, JHPD members requiring personally identifiable information for a criminal investigation must obtain a warrant, court order, or subpoena before accessing SIS. Request to access information must be made through the chain of command to the Operations Commander prior to obtaining the warrant, court order, or subpoena.
- If not providing advance notice to the student, the member requesting the subpoena, warrant, or court order must state in the subpoena or court order that advance notification is not to be made to the student, and the reasons why.

C. If an outside law enforcement agency or other third party is requesting information about a student that is not available on the Johns Hopkins homepage directory, then the JHPD member will advise the agency that a warrant, court order, or subpoena is required, unless a verified health or safety emergency exists.

- If a verified health or safety emergency exists, the JHPD member will request permission from the Chief of Police or their designee, who will coordinate the release of any education records through the Registrar's Office, if appropriate, after consultation with the Office of the Senior Vice President and General Counsel.
- If an outside agency presents the JHPD with a subpoena or court order for student records, the member shall direct the outside agency to the Office of the Senior Vice President and General Counsel for service.
- No JHPD member shall accept service or furnish any records related to a subpoena or court order, as the JHPD is not authorized to accept process for any FERPA information.
- Only the Office of the Senior Vice President and General Counsel may accept service of any subpoena or court order directed to the university.
- The supervisor will ensure notification to the Investigations Division Commander and to the Chief of Police through the chain of command of the subpoena or court order, and any additional information obtained from the requesting agency.

D. Members will only use student personally identifiable information consistent with the following table:

Student Information	Johns Hopkins Directory	SIS
JHPD routine use of student address	Yes. At any time, members may access the Johns Hopkins directory for information	No
Health and safety emergency (JHPD or other law enforcement agency), if approved by Chief of Police and General Counsel		Yes
Criminal investigation or informational use (JHPD or other law enforcement agency)		Only with court order or subpoena, service referred to JHU Senior Vice President and General Counsel
Third-party request		Only with Court Order or subpoena, service referred to JHU Senior Vice President and General Counsel

E. Access to SIS: The Deputy Chief of Support Services will ensure only those with permission and a need to know have access to SIS for health and safety emergencies within the JHPD.

XVI. Patient Record Privacy

A. The JHPD is committed to maintaining compliance with HIPAA to protect patient information by following strict access and disclosure procedures.

B. JHPD members will protect patient confidentiality, including both medical and personal information, from unauthorized disclosure. At no time will any member request or, if known, provide any PHI about a patient of JHHS or JHU medical school clinical services to anyone without meeting the HIPAA privacy rule guidelines and gaining supervisory approval.

C. The HIPAA privacy rule guidelines allow only the minimum necessary information for a law enforcement purpose to be used or disclosed as follows:

- As required by law (i.e., warrant, court order, mandatory reporting, etc.),
- For health care operations (i.e., performing security functions),
- For administrative requests (i.e., investigative request),

- To identify or locate a suspect, fugitive, material witness, or missing person,
- For information about a victim or suspected victim of a crime, or
- To prevent or lessen a serious and imminent threat to the health or safety of an individual or the public.

D. Outside Law Enforcement Requests for PHI

Any member receiving a request for PHI must forward the request immediately to their supervisor. The supervisor must:

- Verify the identity of the requesting individual (appropriate credentials),
- Determine the nature, timing, and extent of the request,
- Forward the request to JHU's Office of the Senior Vice President and General Counsel, which will evaluate the request and coordinate the appropriate response with clinical services or the JHHS Office of General Counsel, when necessary, and
- Refer the outside agency to the Hospital Information Desk or contact the JHHS Compliance Office (or On-Call Administrator after-hours) for additional requests.
- All PHI disclosure requests will be recorded in an Incident Report as an "Assist Outside Agency." The report should include:
    - The exact PHI requested,
    - If disclosed, who approved the discloser,
    - The name and association of the person receiving the information,
    - Date of disclosure and purpose of disclosure, and
    - Any written documentation of the request and approval.

XVII. HIPAA or FERPA Violations

A. If at any time, a member of the department feels there has been a breach in HIPAA or FERPA privacy rules resulting in unauthorized or inappropriate use, disclosure, or access of PHI or education records, they should report the breach immediately to their supervisor and chain of command, who will notify the appropriate compliance office and refer the matter to PSAU.

Policy Enforcement

Enforcement	JHPD managers and supervisors are responsible for enforcing this Directive.

Reporting Violations	Suspected violations of this Directive should be reported to PSAU.

Related Resources

University Policies and Documents
Administrative Procedure # 222, Clery Act Compliance
Personnel Procedure #350, Complaints Against Police Personnel
Operational Procedure #424, Arrests & Alternatives to Arrest
Operational Procedure #426, Interactions With Youth
Operational Procedure #442, Traffic Control & Enforcement
Records Retention and Destruction (GOV029)
Employee Indemnification and Defense (GOV015)
External Documentation
Police Department Forms and Systems

Contacts

Subject Matter	Office Name	Telephone Number	Email/Web Address
Policy Clarification and Interpretation	Policy Management	(667)306-8618	jhpdpolicyinquiry@jh.edu