SUNY COLLEGE OF OPTOMETRY
UNIVERSITY EYE CENTER®

Policy and Procedure:	**Breach of Patient Confidentiality, Report and Notification of**		
Procedure Number:	**B-2**	**Page:**	**1 of 4**
Effective Date:	**2/8/2010**	**Revised:**	**2/24/2026**
Last Reviewed:	**2/24/2026**		

Background:

The University Eye Center (UEC) is entrusted with demographic, financial, and other protected patient information. The patient's record is highly confidential and must be treated with great respect and care by any individual with access to this information. A breach of confidentiality is defined as violating the provisions of UEC's Confidentiality Policy. Any breach of confidentiality by employees may be subject to formal disciplinary action as set forth in this policy.

Policy:

All employees and students are required to report, within 24 hours of discover, any possible incident of inadvertent disclosure or unauthorized access of Protected Health Information (PHI) that may constitute a Breach. Based on the nature of the report and the assessed risk to the patient, remediation and mitigation measures will be implemented as warranted by the investigation's outcome.

Procedure:

A. Reporting

1. The employee must report any possible violation of UEC privacy and/or security practices/policies or breach of patient confidentiality to their immediate supervisor or designee immediately or soon as practical within 24 hours of the occurrence.
2. To the extent possible, the employee and/or their supervisor is expected to initiate immediate action as necessary to prevent further occurrence if the incident is ongoing.
3. If the immediate supervisor or designee is not available or circumstances do not allow, the employee must contact the UEC Privacy Officer by e-mail.
4. In cases in which a breach of UEC clinical information systems is suspected, the employee must contact the Privacy Officer who will contact the Information Security Officer.
5. A confidential report can also be filed by calling the UEC's compliance number at 1-888-906-6777 or via email at privacy@sunyopt.edu. The Compliance Officer will forward any confidentiality issues to the Privacy Officer.
6. Supervisors receiving a report from an employee or directly from a patient or patient's family concerning a possible violation of patient privacy must contact the Privacy Officer immediately.
7. UEC will not take retaliatory action against any employee for reporting a suspected or witnessed violation of privacy policies/procedures or breach of patient confidentiality.

8. The identity of the employee filing a report will not be disclosed unless such disclosure is required for the investigation or remediation process.
9. Employees reporting possible violation of privacy will not be asked to waive their right to file a complaint with the Secretary of the Department of Health and Human Services as a condition of employment.
10. Reports or complaints received by UEC employees from external individuals or agencies alleging a breach of confidentiality or privacy must be directed to the Privacy Officer.

B. Investigation

1. The Privacy Officer will document the details of the report and commence an investigation.
2. The Offices of University Police, Human Resources, Information Technology, and UEC Administration will be contacted to collaborate in the investigation process if the report alleges a violation of privacy policies/practices or breach of confidentiality by an employee, as applicable.
3. A risk analysis will be performed to determine potential harm caused by the incident to the patient and the necessity under applicable laws for notification to the patient and government agencies. The Privacy Officer and/or Information Security Officer will provide the results of the Breach Notification Risk Assessment to the appropriate parties.
4. If it is determined that a breach has occurred, pursuant to the NYS Security Breach and Notification Act, the Information Security Officer will follow the campus Information Security Breach and Notification procedures will report the incident to the proper authorities.

C. Remediation and Mitigation

1. The Privacy Officer will mitigate, to the extent reasonable, any harmful effect to the patient resulting from the use or disclosure of protected health information in violation of UEC's privacy policies or procedures.
2. If it is determined that the personal information at issue was unsecured, the result of an unauthorized acquisition, access, use, or disclosure, and poses a significant risk to the financial, reputational, or other harm to the patient the following will occur:
   - The patient(s) will be sent a plain-language notification letter by first-class mail to the last known address notifying them of the incident, actions to protect the individual from misuse of the information, and actions taken by the organization to prevent or minimize future like occurrences.
   - If the incident involves more than 500 individuals, the applicable government agencies will be notified by the VP for Clinical Administration. The Director of Communications will be the authorized person to contact the media or consumer agencies regarding a breach, as applicable.
   - If contact information is out-of-date or insufficient for 10 or more patients, substitute notification will be placed in a conspicuous location on the UEC's website and may also be placed in media print in geographic areas where the patient(s) affected likely reside.

- Incidents involving more than 500 individuals must be reported to the Secretary of the Department of Health and Human Services (HHS) no later than 60 calendar days from end of the previous year as per HHS regulations.

3. Action will be initiated by the Privacy Officer to facilitate remediation of future occurrences of such violation or breach based on a root cause analysis of the contributing factors.
4. Sanctions will be applied as appropriate to employees violating UEC privacy policies and procedures, as determined by the investigation process;
    a. As outlined under applicable contractual agreements and/or bargaining unions
    b. If the individual accused of the breach is a faculty member, the process will be as outlined under applicable contractual agreements
5. Reporting a breach in bad faith or for malicious reasons may be interpreted as a misuse of the reporting mechanism(s) and may result in disciplinary action.
6. Sanctions may include, but are not limited to:
    a. Counseling
    b. Oral Warning
    c. Written Warning
    d. Suspension
    e. Termination
7. Disciplinary sanctions and appeals are handled in accordance with applicable University Eye Center procedures, and the contractual agreement with the employee.
8. University Police and other law enforcement agencies may be notified if it is determined that the action of the employee constitutes possible criminal activity.
9. If a business associate commits the breach or violation and the business associate does not cooperate with remediation efforts, the contract may be terminated and/or the incident reported to the Secretary of HHS.
10. The Privacy Officer will retain documentation of all reports and action taken for a period of six years.

Definitions:

Breach - A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information.

Examples of breaches of confidentiality related to patient care, may include, but is not limited to:

1. Individuals discussing patient information in any public area;
2. An individual leaves a copy of patient medical information in a public area;
3. An individual leaves a computer unattended in an accessible area with a patient record unsecured;
4. Failure to log off the computer terminal in patient accessible area;
5. Sharing or exposing passwords;
6. An individual looks up birth dates, addresses of friends or relatives, or requests another individual to do so;
7. An individual accesses and reviews the record of a patient out of concern or curiosity, or requests another individual to do so;
8. An individual reviews the record of a public personality or requests another individual to do so;

9. An individual reviews a patient record to use information in a personal relationship;
10. An individual reviews the patient record of a public personality for the intent of giving or selling information to the media;
11. An individual reviews confidential information of another employee who is also a patient;
12. An individual reviews confidential information that may bring harm to the organization or individuals associated with it.