ADM 403
Security Policy #3

Security Incident Procedures

Purpose of Policy

The purpose of the policy is to develop the response to and reporting of security incidents, including the identification of and response to suspected or known security incidents, the mitigation of the harmful effects of known security incidents, to the extent possible, and the documentation of security incidents and their outcomes.

Definitions

Breach

Breach means the acquisition, access, use, or disclosure of personally identifiable information (PII) or sensitive college data such as email, employee information, confidential information, etc. which compromises the security or privacy of the PII or sensitive college data.

Unsecured PII

Unsecured PII means PII that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology such as encryption. The definition of unsecured PII varies between different federal and state regulations.

Reporting and Response

1. The College will ensure that all incidents, threats, or violations that affect or may affect the privacy, confidentiality, integrity, or availability of PII and sensitive college data will be reported and responded to.

2. The College shall have a Security Incident Response Team (SIRT) charged with the responsibility of identifying, evaluating and responding to security incidents. The Privacy Security Officer shall oversee the activities of the SIRT.

    a. The SIRT will be responsible for investigating all known or suspected privacy and security incidents.

b. The SIRT will document a procedure for all employees to follow to report privacy and security incidents**. See MC Security Incident Response Checklist (only available in hard copy with security officers)** and See **Appendix–F Security Incident Response Log**

c. The College will ensure that all employees receive training on how to identify and report security incidents.

d. All employees must follow the documented procedure to report security incidents. In addition, employees must report all known or suspected security incidents.

e. The SIRT team should communicate by cell phone and not use voice over phone.

f. All employees must assist the SIRT with any security incident investigations.

Breach Determination

The Security Incident Response Team (SIRT) will investigate all reported and suspected security breaches. The SIRT will refer to federal or state regulations and college insurance company attorney recommendations to help with breach determination. Breach determination varies between federal regulations such as HIPAA and GLBA. In addition, breach determination varies significantly between state regulations (for example, what may be considered a breach in one state may not be a breach in another state).

Breach Notification

If the SIRT determines that a breach of unsecured PII has occurred, breach notification of affected individuals may be required. The SIRT will refer to federal or state regulations, and college insurance company attorney recommendations to help with breach notification requirements. Breach notification requirements varies between federal regulations such as HIPAA and GLBA. In addition, breach notification requirements varies significantly between state regulations (for example, one state may have breach notification requirements that varies significantly from breach notification requirements in another state).

Key elements of a breach notification include:

I. Date of discovery

Usually a breach will be treated as discovered as of the first day the breach is known or by exercising reasonable diligence would have been known.

II. Timeliness of notification

The College will provide the required notifications without unreasonable delay after discovery of a breach. The amount of time The College has to notify affected individuals varies between federal and state regulations and College insurance attorneys will assist in making this determination.

III. Content of notification

If required, a notification will be provided to each individual affected by the discovered breach. The notification should include the following:

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
- A description of the types of unsecured PII that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number or other types of information were involved);
- Any steps individuals should take to protect themselves from potential harm resulting from the breach;
- A brief description of what The College is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
- Contact procedures for individuals to ask questions or learn additional information, which should include a telephone number, an e-mail address, Web site, or postal address.
- The notification should be written in plain language.

IV. Methods of notification

Methods of notification will be determined by federal and state regulations or any other legal requirements and college insurance company attorney recommendations.