The VMC Privacy Office coordinates compliance with the required notification steps and prepares the necessary notification and reporting documents. The business unit from which the breach occurred covers the costs of production and mailing of the required notification and any mitigation efforts deemed to be appropriate.

I. Breach of Protected Health Information (PHI)

A. When the Privacy Office is notified or otherwise becomes aware of an event involving known or suspected unauthorized acquisition, access, use, or disclosure of PHI; an investigation internal to VMC is conducted to determine if:
   1. VMC privacy and/or information security policies have been violated; and/or
   2. PHI has been accessed, used, or disclosed in a manner that violates the HIPAA Privacy Rule; and
   3. Breach notification is required.

B. Confirmed violation of privacy and/or information security policy results in disciplinary action consistent with the VMC policy for Sanctions for Privacy and Information Security Violations (OP10-40.32).

C. Violations of the HIPAA Privacy Rule are evaluated to determine whether the federal definition of “breach” has been triggered. A Breach Notification Analysis form is completed for each such violation. The Breach Notification Analysis will identify whether the additional Assessment of the Risk of Harm to the Individual needs to be documented using the Risk Assessment Scoring Grid. All documentation related to these analyses is retained for six (6) years.

D. Based upon the above noted Assessment of the Risk of Harm, those incidents that trigger the federal definition of breach of PHI require the following notification and reporting actions:
   1. Notification to the individual whose unsecured PHI has been or is reasonably believed to have been accessed, acquired, or disclosed as a result of the breach.
   2. Notice to the Secretary of DHHS (Secretary) shall be provided as defined in regulations defined by DHHS:
a) The Privacy Office maintains a log of each breach event that involves less than 500 individuals. Annually the log is reviewed by the Information Privacy and Security Executive Committee prior to being submitted to the Secretary within sixty (60) days of the end of the calendar year.

b) The Privacy Office, after consultation with the Chair of the Information Privacy and Security Executive Committee and the business leader involved in the investigation of the breach, will notify the Secretary immediately of any breach event that involves 500 or more individuals.

c) The Secretary posts to a public Internet website of DHHS a list that identifies each covered entity involved in a breach in which unsecured PHI of more than 500 individuals is acquired or disclosed.

E. Requirements for Notification to the Individual(s):

1. **Timeliness**: notification to the individual must be made without unreasonable delay and in no case later than 60 calendar days after the date of discovery of the breach.

2. **Method of notice** must be provided promptly and in the following form:

   a) Written notification by first-class mail to the individual (or the next of kin of the individual if the individual is deceased) at the last known address of the individual or the next of kin, respectively, or, if specified as a preference by the individual, by electronic mail. The notification may be provided in one or more mailings as information is available.

   b) In the case in which there is insufficient, or out-of-date contact information (including a phone number, email address, or any other form of appropriate communication) that precludes the above described written notification to the individual, a substitute form of notice shall be provided, including, in the case that there are 10 or more individuals for which there is insufficient or out-of-date contact information, a conspicuous posting for a period determined by the Secretary on the home page of the Web site of the covered entity involved or notice in major print or
broadcast media, including major media in geographic areas where the individuals affected by the breach likely reside. Such a notice in media or web posting will include a toll-free phone number where an individual can learn whether or not the individual’s unsecured protected health information is possibly included in the breach.

c) Notice to prominent media outlets is required following the discovery of a breach if the unsecured PHI of more than 500 residents is, or is reasonably believed to have been, accessed, acquired, or disclosed during such breach. VMC News and Public Affairs coordinates placement of this notice with media outlets.

d) In any case deemed to require urgency because of possible imminent misuse of unsecured protected health information, the individual(s) may be contacted by telephone or other means in addition to, but not in place of, the required notification noted above.

3. **Content of Notification**: regardless of the method of notice, the notice of a breach includes, to the extent possible, the following:

a) a brief description of what happened, including the date of the breach and the date of the discovery;

b) a description of the types of unsecured PHI that were involved (such as full name, Social Security number, date of birth, home address or phone, etc.);

c) the steps the individual should take to protect themselves from potential harm resulting from the breach;

d) a brief description of what is being done to investigate the breach, to mitigate losses, and to protect against any further breaches; and

e) information about contact procedures for individuals to ask questions or learn additional information, including a toll-free telephone number, an e-mail address, Web site, or postal address.
II. Computerized Data Security Breach of Personal Information (Reference Flow Chart):

A. When VMC information technology and security management professionals have reason to believe that computerized data has been hacked, stolen, lost or otherwise compromised, the VMC authorities responsible for collecting, maintaining, and storing the data will be consulted to determine whether or not Personal Information was resident in the system or on the device that was accessed.

1. If Personal Information was not present, then notification is not required.

2. If Personal Information was present, then VMC determines whether or not the data was encrypted.

B. If any of the Personal Information was not encrypted, then the information technology and security management team determine whether or not there is reasonable belief that any Personal Information was acquired or under the control of an unauthorized individual, system, or device.

1. When the device or computer resides behind a firewall with a perimeter intrusion detection system:
   
   a) and the perimeter intrusion detection system confirms that data did not leave VUMC control, then notification is not required, but
   
   b) if the perimeter intrusion detection system is not able to confirm that data did not leave VMC control, then notification to the individuals whose Personal Information may have been compromised is completed in accordance with the notification requirements defined below.

2. When the device or computer does not reside behind a firewall with a perimeter intrusion detection system:
   
   a) if there is no indication of unauthorized acquisition or control of data, then notification is not required; but,
   
   b) if there is reasonable belief that data may have been subject to unauthorized acquisition or control, then notification to the individuals whose Personal
Information may have been compromised is completed in accordance with the notification requirements defined below.

C. The VMC Privacy Office is notified when there is reasonable belief that a Computerized Data Security Breach of Personal Information has occurred. The Privacy Office will consult with the VMC business leader responsible for the data and confirm whether or not notification is required and, if so, what type of notification response is appropriate based upon the above defined factors. If consensus is not clear or if the business leader believes an exception to the above processes is appropriate, then a final determination will be made by the core executive members of the Information Privacy and Security Executive Committee.

D. Notification Method and Timeframe:

1. Notification requirement – with confirming evidence: When data confirms a Computerized Data Security Breach, then affirmative written notice will be provided to the individual(s) whose Personal Information may have been involved:

   a) Notice will be delivered by mail using notification letter “Type A: With Confirming Evidence” unless the individual has given VMC prior written informed consent to electronic notification. (see web references)

   b) If the cost of providing mailed written notice exceeds $250,000 or the affected number of individuals involved exceeds 500,000 or insufficient contact information is available to deliver written notice, then substitute notice is provided by:
      i. Email notice, when an email address is available; and
      ii. Conspicuous posting of the notice on the VMC website page(s); and
      iii. Notification to major statewide media.

   c) If more than 1,000 persons are subject to notification, all three major consumer credit bureaus are also notified.

2. Notification requirement – with no confirming evidence: When VUMC identifies a data security incident or event that creates reasonable belief that a Computerized Data Security Breach
has occurred and in the absence of confirming evidence to the contrary, precautionary notice is provided to the individual(s) whose Personal Information may have been compromised:

a) If VMC is able to discretely define the individuals impacted, then written notice will be delivered by mail using notification letter “Type B: Precautionary, No Confirming Evidence”.

b) If the population impacted is not discretely defined or if sufficient contact information is not available, then notification may be provided by:
   i. Email notice, when an email address is available; and
   ii. Conspicuous posting of the notice on the VMC website page(s).

3. Notification timeframe: Notification will be provided within the most expedient time possible and without unreasonable delay, but delay may be appropriate for:

a) Measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system; or

b) To support the needs of a criminal investigation if a law enforcement agency determines that notification will impede the investigation.

III. Additional Notice and Mitigation - Indication of Identity Theft:

When VUMC becomes aware that data secured through a Computerized Data Security Breach has been used by an unauthorized person for a specific purpose, such as to commit identity theft, then additional affirmative notification and mitigation steps are implemented as follows:

A. Written notice identifying the probable risk of identity theft is delivered by mail using notification letter “Type C: Mitigation Steps Recommended”, or

B. Substitute notice as described above in B. 1.b. is acceptable if the costs and number of individuals exceeds the defined limits or if insufficient contact information is available to deliver written notice by mail.
C. A VUMC hotline telephone number is also established to handle questions, and

D. If more than 1,000 persons are subject to notification, and reporting to the three major consumer credit bureaus has not already occurred, then all three major consumer credit bureaus are also notified.

E. VUMC provides additional mitigation, such as identity theft recovery services on a case-by-case basis.