The Maine Data Act

The Notice of Risk to Personal Data Act (the Act) (10 M.R.S.A. § 1346 et seq.) creates a duty to investigate breaches in the security of an individual’s computerized data and an obligation to notify such individual of the breach in specified situations.

A breach is defined as an unauthorized acquisition of data “that compromises [its] security, confidentiality or integrity,” or an authorized acquisition which is then used for an unauthorized disclosure of such Personal Information. For the purposes of the Act, the data protected is referred to as “Personal Information” stored in a University storage system. That is: An individual’s first name, or first initial, and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

A. Social security number;
B. Driver’s license number or state identification card number;
C. Account number, credit card number or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes or passwords;
D. Account passwords or personal identification numbers or other access codes; or
E. Any of the data elements contained in paragraphs A to D when not in connection with the individual’s first name, or first initial, and last name, if the information if compromised would be sufficient to permit a person to fraudulently assume or attempt to assume the identity of the person whose information was compromised.

Personal Information does not include “publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.” Someone “unauthorized” is a person who “does not have authority or permission to access the information... and/or obtains access by fraud, misrepresentation or similar deceptive practices.” If the University becomes aware of a breach, it must “conduct in good faith a reasonable and prompt investigation to determine the likelihood that Personal Information has been or will be misused.” If, after the investigation, it is determined that a covered breach has occurred, notice must be given to the person(s) affected. It must contain the date of the breach; the information believed to have been accessed, a summary of the University’s response to the breach and a person they can contact for additional information. The notice must be given as “expeditiously” as possible and “without unreasonable delay,” consistent with the needs of law enforcement and the need to restore the reasonable integrity, security and confidentiality of the data in the system. Notification is required when personal information was or is reasonably believed to have been acquired by an unauthorized person...and there is likelihood that it will be misused. Notice must be in writing (presumably given by U.S. Mail) to the person’s known address unless the cost would exceed $5,000 or notification has to be given to more than 1,000 people. In these events or if there is no mailing address available “substitute notice” can be given by both e-mail and also placed conspicuously on the University’s website. If substitute notice is given, the statewide media must also be notified.