YOUR LEGAL OBLIGATIONS IN REPORTING A DATA BREACH

If your organization believes it may have experienced a data breach involving either health information or personally identifiable information, it is critical to follow the steps in reporting the breach to the proper regulatory bodies and/or notifying affected individuals.

- **A breach involving health information** is overseen by a federal regulatory bodies, such as the Department of Health and Human Services (HHS) and the Office for Civil Rights (OCR).*

  HHS has specific federal rules that must be followed in response to a data breach:

  1. Notification must be made to the affected individual without unreasonable delay, and no later than 60 days post discovery. Typically, the notification needs to be via first class mail unless an address is not available or the affected individual has consented to email notification.

  2. Breaches involving 500+ individual records also require a notice to HHS/OCR without unreasonable delay and no later than 60 days post discovery. This notification can be made via the HHS website. Breaches involving less than 500 individual records must be reported on an annual basis at the end of the calendar year on the HHS/OCR website. The deadline for this reporting is no later than 60 days after the end of the calendar year.

  **** Note -*** *While the OCR and the HHS are currently the two most active regulatory entities overseeing organizational data breaches, there are others with the authority to do so. Depending on the nature of the organization and severity of the breach, there is precedent for entities such as the Federal Trade Commission (FTC), Securities and Exchange Commission (SEC) and Office of Homeland Security to intervene. Until there is widespread federal data breach legislation passed denoting governing responsibility, ambiguity among governing bodies will remain*.

- **Notification requirements for general (Non-health) related personally identifiable information** (name, address, social security number, financial information) are overseen by individual states. An organization must follow the notification rules and requirements of the state(s) in which each affected individual resides.

  The difference between personally identifiable information and health information is not clear cut. Health information generally includes personally identifiable information and, often, this information is the only sensitive part of a health record. However, it is classified as a health record when used in conjunction with a medical record or history.

Contact your M3 professional for additional assistance understanding your reporting requirements in response to a data breach.