WHAT HAPPENS WHEN YOU REPORT A DATA BREACH?

- UWM’s Information Security Office will assist you.

- UWM’s Information Incident Response Procedure details steps to be taken in the event of a breach.

- UWM’s response will vary based upon the type of confidential information involved, how many people are affected, and UWM’s reporting/notification obligations.

- If necessary, an Information Incident Response Team (IIRT) will be formed with representatives from the affected campus area and, as needed, representatives from Internal Audit, the Office of Legal Affairs, the Information Security Office, University Relations, Risk Management, the CIO, HIPAA Privacy Officers, and the UWM Police Department.

- The IIRT will consult as needed with UWM Administration including the Provost, Vice Chancellors and other experts.

- The IIRT will also work with the affected area to mitigate any harm, put in place steps to protect against future breaches and send out any required notifications to affected individuals.

UWM INFORMATION INCIDENT RESPONSE TEAM

INFORMATION SECURITY OFFICE: 414-229-1100

CHIEF INFORMATION OFFICER: 414-229-3713

INTERNAL AUDIT OFFICE: 414-229-5586

OFFICE OF LEGAL AFFAIRS: 414-229-4278

RISK MANAGEMENT: 414-229-5079

UNIVERSITY POLICE: 414-229-4627

UNIVERSITY RELATIONS: 414-229-4035

Report all suspected or confirmed/known unauthorized disclosures of confidential electronic or paper information to:

UWM Information Security Office
414-229-1100 or infosec@uwm.edu

Additional information is available at: security.uwm.edu
WHAT IS A REPORTABLE DATA BREACH?
Any occurrence that could potentially result in unauthorized access to confidential UWM information, including electronic and paper records.

The following are examples:
- Loss or theft of computers, electronic devices and media or paper files, where it is reasonable to believe confidential information was present and unauthorized individuals could access confidential information.
- Intrusion by malware or other unauthorized access via any network into computer systems.
- Unauthorized entry into offices, files, desks, or work areas, where it is reasonable to believe that confidential information was accessed by unauthorized persons; or
- Any other circumstances where it is reasonable to believe that confidential information may have been accessed by unauthorized persons.

WHAT AM I REQUIRED TO DO?
Any breach (suspected or confirmed/known) of UWM confidential information/data must be reported to the UWM Information Security Office at 414-229-1100 or infosec@uwm.edu.

Individuals who suspect that unauthorized access may have occurred should notify their supervisor and/or head of the affected area who in turn should call the UWM Information Security Office. If you are not sure who to notify, call the Information Security Office directly.

WHAT IS CONFIDENTIAL INFORMATION?
Confidential information covers a wide array of information and includes:
- Social Security numbers
- Credit card numbers
- Bank account numbers and other financial account numbers
- Driver’s license or state ID number
- Individual’s DNA or biometric identifier
- FERPA (student) data
- HIPAA (personally identifiable patient health) data

WHAT IF I AM NOT SURE IF CONFIDENTIAL INFORMATION WAS ACCESSED?
You should call the UWM Information Security Office. It’s their job to help you figure out if information has been accessed and if so, whether confidential information was involved. When in doubt—call.

DOES UWM HAVE A POLICY OR PROCEDURE TO DEAL WITH DATA BREACHES?
Yes, UWM has an Information Incident Response Procedure which allows it to quickly and systematically respond to data breaches.

UWM’s response to any given compromise will vary based on circumstances. However, the University will always:
- Work to protect any compromised information/data as quickly as possible;
- Put in place appropriate mitigation measures; and
- Comply with any reporting and/or notification requirements and deadlines.