WHAT TO DO
If you DISCOVER an Information Security or Privacy INCIDENT

1 REPORT
Report the incident to the appropriate Delegated Authority

THE CLOCK IS TICKING!
DO NOT attempt to manage the incident yourself. Before doing anything else, report suspected incidents to one of the delegated authorities listed below depending on what type(s) of data are involved. When applicable, include your management or IT support person.

IF IT IS DETERMINED THAT NOTICATION IS REQUIRED, STATE LAW REQUIRES NOTIFICATION TO THOSE AFFECTED WITHIN

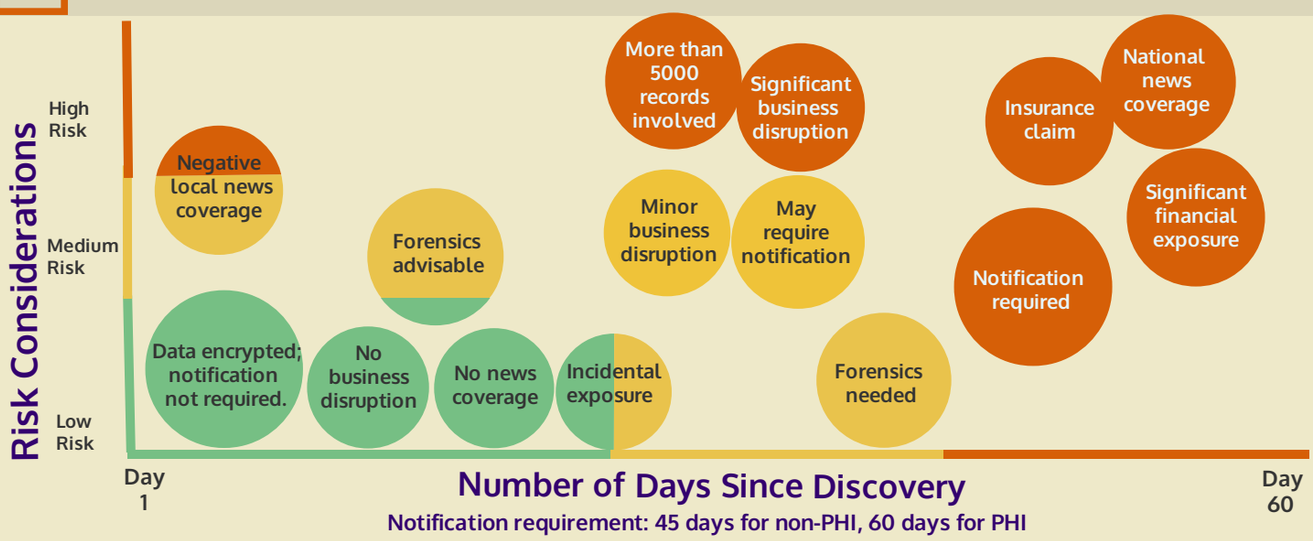
45-60 DAYS
(Depending on data type)

Delegated Authority	Data Type/Area of Responsibility	Contact Information
University Chief Information Security Officer	All information, information systems, and infrastructure technology except for the areas specifically listed below	(206) 685-0116 or ciso@uw.edu or security@uw.edu
Executive Director, Health Sciences Administration	Protected health information (PHI) for Health Sciences Healthcare Components	(206) 543-7202 or hsaea@uw.edu
Chief Compliance Officer, UW Medicine, and Associate Vice President Medical Affairs, UW	PHI for UW Medicine Healthcare Components	(206) 543–3098 or comply@uw.edu
Assistant Director of Regulatory Affairs, Human Subjects Division, Office of Research	Human Subjects Information	(206) 543-0098 or hsdinfo@uw.edu
Empowered Official, Office of Research	Export Administration Regulation and International Traffic and Arms Regulations	(206) 543-4043 or export@uw.edu

2 INFORMATION GATHERING
Promptly report what you know. Delegated authority will substantiate facts, perform forensics, and gather supplemental information. Report the following information:

1. When did the event occur?
2. How many records are involved?
3. Was the data encrypted?
4. What system(s), if any, are involved?
5. What organization(s) or unit(s) are involved?
6. Are there system logs that need to be preserved?
7. Is the system(s) deemed critical to operations?
8. When applicable, inform your management or IT support person.

3 RISK ASSESSMENT
Delegated authority will assess these and other risks:



Notification requirement: 45 days for non-PHI, 60 days for PHI

4 NOTIFICATION DECISION

Delegated authority will determine if notification is required and work with you to develop an action plan.

IS NOTIFICATION REQUIRED?

YES

NO

5 NOTIFICATION

Follow appropriate laws, regulations, and policy.

Non-PHI: 45 days
PHI: 60 days

6 RECORDS MANAGEMENT

Document incident in written form and keep records according to UW retention schedule.