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

**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 NOTIFICATION IS REQUIRED, STATE LAW REQUIRES NOTIFICATION TO THOSE AFFECTED WITHIN 45-60 DAYS**
(Depending on data type)

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

**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.

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

- **High Risk**
  - Significant financial exposure
  - Significant business disruption
  - Insurance claim

- **Medium Risk**
  - Minor business disruption
  - Forensics needed
  - May require notification

- **Low Risk**
  - No business disruption
  - No news coverage
  - Incidental exposure
  - Forensics advisable
  - Data encrypted; notification not required

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

**NOTIFICATION**

- **YES**
  - Follow appropriate laws, regulations, and policy.
  - Non-PHI: 45 days
  - PHI: 60 days

- **NO**
  - Document incident in written form and keep records according to UW retention schedule.

**NOTIFICATION REQUIREMENT**

- **More than 5000 records involved**
- **Significant business disruption**
- **Insurance claim**
- **National news coverage**
- **Significant financial exposure**

**NUMBER OF DAYS SINCE DISCOVERY**
Notification requirement: 45 days for non-PHI, 60 days for PHI

**RECORDS MANAGEMENT**
Office of the Chief Information Security Officer
University of Washington
ciso.uw.edu/report
More info: UW APS 2.5, Information Security and Privacy Incident Reporting and Management Policy