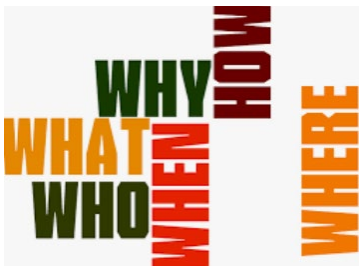
Step 1: Discovery and Fact Finding - The Discovery & Fact Finding phase is where the process begins, and the privacy incident is first acknowledged and then reported through the Privacy Incident/Complaint form and submitted to the Compliance and Privacy Office (CAP).***The date of DISCOVERY determines the 60-day reporting timeline and is very important***.

Step 2: **Contact Helpdesk immediately (512-854-9175)** if a device needs to be disabled to *contain the incident*. (Not all incidents require devices being disabled), then report the incident to the **Compliance and Privacy Office (CAP); CAP's number is 512-854-1114.**

Step 3: **Investigation, Analysis, and Determination** - After discovery and fact finding, contacting Helpdesk and CAP, immediately gather the following items:

- Date of Discovery
- Discovered By Who?
- Discovered How?
- Reported By?
- Employee Involved – all contact information
- Device Asset Tag Number
- Description of the incident and why you think it may be a unauthorized disclosure of information
- Has the employee in question been questioned?



The involved staff member will need to be officially interviewed by the CAP Office to gather additional facts and provide any information or evidence to aid in the investigation.

The CAP Office will conduct an investigation, do an analysis of the data and evidence, and *determine the level of impact*:

- Low
- Med
- High

Step 4: **Status Updates** - The Compliance and Privacy Office (CAP) will provide updates to leadership and all parties involved when applicable throughout the investigation.

Step 5: **Corrective/Disciplinary Actions**; Per Policy 1.7 Corrective/Disciplinary Actions; it states that CAP should recommend the appropriate Corrective/Disciplinary Actions which may include retraining, modification and/or termination of contracts or modification and/or termination of volunteer agreements. ***The final decision is always at the discretion of the department***.

Step 6: **Official Notification to Victims/Mediations** - The Compliance and Privacy Office (CAP) will send out disclosure notification letters to the affected victims (by first class mail), if any, and work with Risk Management to address any 3rd party services needed. Mediation Example: Life Lock (1 year credit monitoring service).

Step 7: **Remediations/Lessons Learned for effected Departments** - The Compliance and Privacy Office (CAP) will work with departments regarding the remediations to prevent reoccurrence of the incident.
Examples of Remediations:

- One on One Coaching/Department Mentorship
- Refresher Training
- Policy and Procedure Revisions

Step 8: **Conclusions/Final Report** of the investigation results are shared and reviewed with department management and the staff member involved.

Step 9: **Report to Outside Authorities (501+)** - The Compliance and Privacy Office (CAP) will communicate to Commissioners Court, and report to outside authorities (Office of Civil Rights (OCR)/Office of Inspector General (OIG) if applicable, based on the impact/cause, severity, and the number of records (501+) that were disclosed.

Step 10: Closeout Briefing (if applicable) - The Compliance and Privacy Office (CAP) will provide a final opportunity to answer any questions from leadership, management, or any staff members before closing out the incident.