



**PLEASE CONTACT YOUR ATIP OFFICE IMMEDIATELY  
IF YOU SUSPECT A PRIVACY BREACH HAS OCCURRED**

A privacy breach involves improper or unauthorized creation, collection, use, disclosure, retention or disposal of personal information

## HOW DO MOST BREACHES OCCUR?

### ACCIDENTAL DISCLOSURE

This may be caused by an inadvertent error on behalf of an employee such as misdirected mail or e-mail

### LOSS OF CONTROL

The theft or loss of equipment, mobile devices, or documents containing personal information

### UNAUTHORIZED ACCESS

Compromised or inadequate security and access controls for information in print or electronic format

## FOLLOW THE PRIVACY BREACH MANAGEMENT TOOLKIT

### RESPONSE

#### ASSESS AND CONTAIN

Once a suspected or known privacy breach has occurred, take immediate action to contain the breach and to secure the affected records, systems, email or websites.

#### CONTACT YOUR ATIP OFFICE

Each institution is required to have plans in place to address privacy breaches. Work with your ATIP Office to coordinate the next steps to respond to the privacy breach.

#### DOCUMENT THE BREACH

Keep records throughout the process as this will help better understand the circumstances that led to the breach.

### PREVENTION

There will always be the risk of a privacy breach, despite everyone's best efforts.



Institutions should:

- review internal policies and procedures
- offer training and education
- review access controls
- encrypt portable electronic devices
- conduct of ongoing monitoring, logging, and audits of physical and technical security

