

Preventing Loss or Theft of Equipment or Data

Physical loss of your equipment (or data that you have access to and work with daily) needs to be carefully protected. The most important thing you need to know is this:

As soon as you realize your device or equipment has been stolen or misplaced, notify your supervisor and IT security professional immediately so appropriate measures can be taken to safeguard the data saved on your device or equipment.

The data saved it is now compromised and susceptible to unauthorized access, dissemination, and use. This is a serious cyber breach and should be handled by trained IT security professionals.

Action—Report

Contact your IT administrator, practice manager, or immediate supervisor.

Any suspicious activity on your system? Add their name and number to this sheet for reference.

Quick action is imperative. This threat is real!

Steps to take

Review this list of best practices and follow each recommendation.



HHS 405(d)
Knowledge on Demand

Tips to protect equipment and prevent data loss:

- Never** leave your laptop or iPad unattended at work or in transit.
- Follow the password policy and update passwords as required!
- Never** share your password with anyone.
- Follow company policy on accessing internet sites.
- Avoid using USB drives on your organization's computer.
- Encrypt sensitive data.
- Report any loss or equipment or suspicious activity on your system **immediately!**
- Alert proper officials immediately if something seems suspicious.
- Keep your emergency contact list close by.

Proactive measures go a long way to protecting yourself and the data you manage.

Reporting

Report to:

Contact Info:

For more resources and to learn more about how you can protect your patients from cyber threats, check out the *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP)* publication at [405d.hhs.gov](https://www.hhs.gov/405d).