Codify
BY AAPC

# Health Information Compliance Alert

## Train Your Employees To Fight Ransomware

One of your best defenses against ransomware is an educated staff, points out new **HHS's Office of Civil Rights** guidance.

A good security training program busts the "it can't happen to me" myth. Teach your employees that many ransomware attacks begin when an employee opens a file from an unreliable source or opens an unexpected attachment on what appears to be a colleague's email message.

Train employees to think before they message, download, or buy. They should open files only if they are from trusted personnel and only if they are expecting the file.

You should all make sure that your staff knows the signs that a device may have been infected or attacked. Teach them to look out for these "red flags" that something has gone wrong. Make sure they know which staffer to contact if they spot these red flags.

*Many unwanted ads pop up frequently.

*System won't start normally. For example, user may see "the blue screen of death."
*Browser goes to unwanted pages automatically.
*User can't control the mouse pointer.
*Anti-virus software doesn't appear to be working.
*User is unable to log into their device.

**Note:** Read the OCR guidance here: https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf.