A WEEK AFTER I got a PDA (personal digital assistant or handheld computer) to use as a pocket drug guide and clinical calculator, I was called to see the nursing supervisor.

“You shouldn’t be using your PDA given the HIPAA privacy regulations,” she told me. Only after I explained that my PDA contained no information that would reveal patients’ identities was she reassured. Do you know if your clinical use of your PDA is in compliance with the law?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that you recognize and protect oral, written, and electronic information that could reveal a patient’s identity and health-related information, also called protected health information (PHI). Any health data that are connected to a patient’s identifying information—names or numbers—are considered PHI.

With violation fines ranging from $100 to $250,000, administrators are understandably concerned about all forms of PHI communication, whether via telephone, census boards, or even nurse-to-nurse conversations. Protecting electronic PHI isn’t difficult, but you need to recognize what’s safe and what’s risky.

Here’s a guide for HIPAA-compliant use of your PDA.

**Green light: Safe data for your PDA**

Most clinical uses of PDAs fall within HIPAA compliance. You can use your PDA safely with drug reference programs, diagnostic test guides, clinical calculators, and decision-support programs. You may need to enter a patient’s weight and height to calculate body mass index, or the name of a test he’s getting, but these data are HIPAA-safe because they don’t identify the patient, and entering data without the patient’s name or identifying number is always safe.

**Yellow light: Caution required**

Use caution when carrying your PDA, transmitting data, or getting repairs. Because it can easily be lost or stolen, get in the habit of putting it in your pocket or in its own holster. Losing your PDA with PHI on it is like losing a patient’s chart.

Data that are sent electronically (“beamed”) from one PDA to another using infrared light usually don’t need encryption. Beamed data can travel only a few feet, making unwanted interception nearly impossible. Just keep the two PDAs within a foot of each other when beaming.

**Red light: Password or encryption required**

In home health care or clinics, nurses are likely to use scheduling or data management programs that store PHI such as patient appointments, history and physical data, lab results, and even photos. One option to block access to that data on your PDA is using a password only you know.

If your PDA is ever sent out for repair or servicing, make sure that you completely erase all patient data from storage first, or consider doing a “hard reset,” which restores the PDA to its original state. Check your PDA’s manual for instructions.

**PHI + PDA = HIPAA**

Remember, if information on your PDA is patient data that you wouldn’t talk about in public or post on a bulletin board, then it’s PHI. Treat PDA PHI as you treat a patient’s medical record, and you’ll be HIPAA-compliant.

---

**INFOBYTES**

**HIPAA guidelines for using PDAs**

BY BRENT W. THOMPSON, RN, DNSc

---

**QUICK GUIDE TO HIPAA-COMPLIANT PDA USE**

**Don’t worry if you’re using:**
- data not connected with identifiers
- clinical reference guides
- decision-support software
- clinical calculators.

**Take precautions:**
- against loss or theft of PDA
- when “beaming” data to another PDA
- before having PDA serviced.

**Always use passwords and/or encryption for:**
- data transmission on network
- synchronizing with desktop personal computer
- patient appointments
- history or physical data
- lab data
- patient demographics or identifiers
- patient photos.