

HIPAA: Dos and Don'ts

There are many common-sense things you can do to protect privacy. Becoming familiar with the new patient rights and OHSU's new HIPAA policies can seem overwhelming at first. Here is a very basic summary of some HIPAA Dos and Don'ts:

Do:

1. Check that the patient was provided with a Notice of Privacy Practices at first delivery of service. This will be documented on a screen in A2K.
2. Understand and respect the patient's right to restrict the communication of health information to friends and family
3. Understand a patient's right to opt out of our facility directory
4. Understand the difference between "authorization" and "informed consent"
5. Give a copy of the signed authorization to the patient
6. Share information with providers for treatment, including outside records in our possession
7. Allow patients to access and obtain copies of their health records
8. Refer patients to HIS if they want health information from multiple OHSU sites
9. Ensure that someone in your area is tracking disclosures subject to the accounting requirement
10. Proactively address patient complaints about privacy breaches

Don't:

1. Agree to restrict uses and disclosures for treatment, payment, and health care operations. Make sure that the patient receives the proper form to make this request, then send it on to the Office of Information Privacy and Security (Mail Code: AD 140).
2. Don't agree to a request for a specified method of communication unless it only involves your service area. Once you've agreed to this kind of request, document it in the patient's chart.
3. Be afraid to ask your supervisor for guidance if you are not sure how to proceed
4. Share your password or log on
5. Forget to log off when you step away from a workstation
6. Feel like you're alone. Many HIPAA resources can be found at www.ohsu.edu/integrity/ips/resources