Objectives:

- Identify the main ethical and legal principles regarding confidentiality and respect for privacy.
- State the circumstances under which disclosing patient information may be ethically permitted and/or legally required (i.e., exceptions to the confidentiality requirement).
- Recognize and discuss commonly occurring problems and barriers to protecting patient privacy.
- Review and discuss specific cases in which confidentiality is at issue.

Required Reading:

Holleman, Medical Ethics, pp. 278-282 (On reserve in McGoogan Library) and this outline of information.

Confidentiality/Privacy Outline:

Keeping information confidential means:

Refraining from disclosing information without the permission of the source of the information.

Health care workers have a professional duty to maintain confidentiality with respect to the information their patients tell them or allow them to discover through testing/examination.

1. Why is confidentiality important?

(a) Adverse consequences of lack of confidentiality:

- Disclosing certain information can significantly harm patients. Patients can lose their jobs, be denied health insurance, become estranged from their families, and suffer social prejudice. Disclosing sensitive
information (e.g., relating to sexual activities/orientation, drug use, mental health, HIV status) is especially likely to cause harm.

- If patients are not confident that their interactions will be held in confidence, they may be inhibited from telling their doctors about important things. This can reduce quality of care. For instance, a patient may withhold items from her medical history, which, if present, would help her doctor treat her.

- Similarly, patients may not seek treatment for sensitive problems if they fear that others will know they did so.

(b) Autonomy

Even if the patient is not harmed in one of the above ways, breaching confidentiality violates the patient’s autonomy. Autonomy is the right to choose for oneself. How does telling your roommate about Mr. Smith’s enormous hemorrhoids violate Mr. Smith’s right to choose for himself? Your roommate doesn’t even know him. It is not obvious how this disclosure limits Mr. Smith’s choices. It does, however: it limits his choices about who gets his information and who does not. That is, you’ve usurped Mr. Smith’s power to direct the flow of information about him.

2. What are the limits of confidentiality?

Sometimes there is good reason to disclose private medical information. Withholding information can put others (or the patient) at great risk for serious harm. Disclosing certain information, for example to an epidemiological researcher, can be very beneficial to society at a minimal risk to the patient. Sometimes health care workers are required by law to disclose information. Here are the conditions under which you may (or must) disclose patient information:

- The patient is incapable of making an informed decision about care and a parent, guardian, or surrogate must assume decisional responsibility.

- Insurance companies that pay for treatment want to know what they are paying for. This may not require disclosing the patient’s entire medical record to the insurer, but it does require passing on certain information. By buying insurance, the patient consents to having her information disclosed to the insurer. However, (a) the patient may not understand how the information flow works, and (b) if the patient cannot afford treatment without insurance, this “consent” is coerced.
• Medical information relating to **violent injuries or the abuse of someone vulnerable** (child or elderly/disabled person) must be reported.

• Certain **communicable diseases must be reported to the local health department** so that their spread can be monitored. Reportable diseases include HIV/AIDS and other STDs, measles, rabies, hepatitis (non-A), leprosy, and the plague. Personally identifiable information is included in these reports (i.e., name and address) but is kept confidential by the health department. For example, when the health department shares HIV information with the Centers for Disease Control, the patient’s name and address are withheld.

• If not disclosing patient information **seriously endangers a specific other person or people**, disclosure is warranted. For example, if a patient refuses to disclose his HIV status to his current (unprotected) sexual partner, you would first try to persuade him to do so, offering help and counseling. But if he still refuses, and you are unsure if the sexual partner will learn of this from the health department reporting system, telling the partner is appropriate. This is a case where (a) the risk to another is significant, and (b) the threat is specific and imminent.

• The **court may subpoena a patient’s medical records**. This usually happens when the patient’s medical condition is an element of a legal claim or defense.

• Patient records may be analyzed as part of a **medical fraud investigation**. Although names can be electronically “hidden,” much specific information about a patient’s medical care is relevant. For example, suppose a health care worker is suspected of billing for undelivered services. The fraud investigation may examine services the patient received from other providers, the patient’s health over a period of time, and where the patient was at various times (e.g., was the patient in an ICU at the time of the supposed services?).

Hospitals and professional groups that **oversee the quality of patient care** need access to patient records so they can assess whether the patients have been treated appropriately.

• Patients’ medical records are used for **biomedical research**. Usually, the names and other identifying information are removed from the records. Sometimes getting the patients’ consent is impractical. For example, pharmaco-epidemiologists survey huge numbers of records to determine
the risks associated with particular drugs. This information is very beneficial to society.

3. **What are the laws and professional standards?**

Case law supports a constitutional right to privacy (variously attributed to Amendments 1, 4, 5, 9, and 14 of the Bill of Rights), and a right to confidentiality in the healing relationship [*e.g.*, Jaffee v. Redmond, *518 U.S.* 1 (1996), protecting the communications of a psychotherapist and client]. However, the rights to privacy and confidentiality are not absolute. Simonsen v. Swenson, *177 N.W.* 831 (1920) upheld the right of a physician to warn a hotel owner that a boarder was syphilitic. Tarasoff v. Regents of University of California, *551 P 2d* 334 (1976) held a psychologist liable for failing to warn a murder victim that his patient planned to kill her. In that case, the court found that the duty to warn arises with a significant risk of severe, irreparable damage to an identifiable third party who could take steps to avoid the risk. "The protective privilege ends where the public peril begins." (*id.* at 347).

The 1983 President's Commission for Study of Ethical Problems in Medicine, Biomedical and Behavioral Research permits (but doesn't recommend or require) disclosure of genetic information to relatives if reasonable attempts to persuade the patient to disclose have failed; there is a high probability of harm to an identifiable third party; disclosure would allow prevention or mitigation of harm; and the disclosure is limited to the information needed to diagnose or treat the condition. A recent New Jersey case [Safer v. Estate of Pack, *677 A 2d* 1188 (1996)], while upholding the physician's duty to communicate the hereditary nature of a diagnosis to a patient, implied that a physician may in some cases have a duty to warn relatives over the objections of a patient.

The Privacy Act of 1974 applied only to information held by federal agencies, and was not specifically aimed at *medical* information. But it did advance the concept of "fair information practices." These practices are: (a) no secret records; (b) there must be a way for people to find out what information on them has been collected and how it is used; (c) information obtained for one purpose should not be used for other purposes without consent; (d) people must be able to correct information about themselves; (e) organizations using information must assure the reliability of the data and prevent misuse.

Currently there is no national legislation covering the confidentiality of medical records. Most states have laws, but these laws are diverse. For example, about 2/3 of the state
laws specifically allow patients access to their own records; some do not specify whether the patient can copy the record or suggest corrections. Nebraska statutes do not specifically address patient access to medical records, however common law supports access. Some state laws are not comprehensive -- they are restricted to specific conditions (e.g., confidential information about AIDS, mental health status). Often, no clear penalties for breaking the laws are given.

The Health Insurance Portability and Accountability Act of 1996 set an August 21, 1999 deadline for Congress to pass a national law protecting the confidentiality of electronic medical records. Failing that, the Secretary of the Department of Health and Human Services was charged with developing administrative regulations to assure the uniformity and the confidentiality of electronically transmitted medical information. Congress failed to act, so the Secretary promulgated regulations, reportedly running in excess of 600 pages. Subject health care plans, providers and clearinghouses must be in compliance by October 2002. In her address to Congress in 1997, Secretary Donna Shalala recommended that a statutory scheme should incorporate the following principles:

(a) Boundaries: With few exceptions, health information must be used only for health related purposes. Even those who have legitimate access to information must restrict their use of the information. For example, an employer who insures employees may legitimately access parts of their health records. But the employer may not use this information to make decisions about hiring, firing, or promotions.

(b) Security: Those holding health information must take all reasonable steps to secure it from illegitimate access (both by employees and external parties).

(c) Consumer Control: The patient has a right to know what is in her record, who else has seen the record, and how to propose amendments to the record.

(d) Accountability: Improper disclosure and misuse of information must be severely punished. Penalties should be more severe for deliberate (e.g., for profit) disclosure, but negligence is also punishable.

(e) Public Responsibility: Confidentiality can be breached in order to support national priorities: public health, research, promoting quality care, and combating fraud and abuse.

Presumably the regulations emanating from HHS aspire to the same goals. It remains to be seen whether the Electronic Transaction Standards will ultimately support or undermine patient rights.
Professional standards regarding confidentiality predate legislation. The Hippocratic Oath contains the following statement:

Whatever, in connection with my professional practice, or not in connection with it, I see or hear, in the life of men, which ought not to be spoken of abroad, I will not divulge, as reckoning that all such should be kept secret.

Modern authors and associations offer professional confidentiality standards that vary in content and complexity (one source lists 28 principles). Excerpts from the American Academy of Family Physicians include:

- The right to privacy is personal and fundamental.
- The privacy of medical information maintained by physicians is privileged.
- The individual should have an appropriate right of access to, and correction of, medical records. [When full and direct disclosure may be harmful, access should be to a designated representative, preferably a physician.]
- The privacy of adolescent minors should not be compromised by granting parents routine direct access to their children's medical records.
- The release of data that is personally identifiable should require explicit patient authorization.
- Any disclosure of medical record information should be limited only to information necessary to accomplish the purpose for which the disclosure is made.
- Disclosure may be made for use in conducting a biomedical or epidemiological research project, or for use in conducting legal medical record audits, provided that stringent safeguards to prevent individual identifiability are maintained.
- No physician should disclose (in identifiable form) any information about the individual without the individual’s explicit authorization, unless (a) the physician is consulting another physician as part of the patient’s treatment, (b) disclosure is made to the next of kin, consistent with accepted medical practice, (c) compelling circumstances affecting the health or safety of an individual dictate disclosure, (d) the physician is reporting certain “reportable” diagnoses to the health department, or (e) a court order or statute requires the release of medical records to a legal authority.
- Any electronic health information systems in which physicians participate should be equipped with appropriate safeguards.

4. What is some practical advice for maintaining confidentiality?

- Adopt a “need to know” attitude. Ask yourself, “Does this person/organization need to know, and, if so, how much does she need to know?” Get in the habit of giving the minimum requested. If disclosing
only part of the record will suffice, do not disclose the whole record unless specifically authorized.

- Obviously, you should not gossip about patients. Less obviously, be aware of the potential for being overheard. Seek private places to discuss patient matters. Do not assume that you cannot be heard behind a closed door -- find out.

- Cellular phones, in addition to being vulnerable to eavesdroppers with scanning equipment, encourage people to have private conversations in public places. Be aware of your surroundings.

- Copiers, fax machines, and printers introduce confidentiality risks -- extra copies discarded insecurely, faxes sent to the wrong places, machinery shared by people who should have access to information and people who should not. Find out about or develop policies for secure use of office equipment.

- Just as you would not leave a patient’s paper record on the table for all to see, do not leave patient files open on your computer when you are not using them. Similarly, in a teaching or conference situation, be sure to erase blackboards and overhead films when you are done.

5. What are some difficult issues relating to confidentiality?

(a) Paper vs. Electronic Records

Medical records no longer reside only in the doctor’s locked file cabinet. They are stored and transferred electronically. This makes people fear that these records will be less secure. Some (e.g., the A.C.L.U.) have proposed that a patient has the right to demand paper-only records. Does the patient have the right to choose the storage medium?

Storing patient information electronically can be beneficial. It might improve the quality of patient care, especially in emergency situations or when multiple providers are involved -- easy access can improve coordination of services. Electronically stored information can be used more easily than paper for research and fraud investigations. And, perhaps, these new storage methods will cut administrative costs.

Do we have to sacrifice confidentiality for these benefits? Probably not. With proper precautions, electronic records can be at least as secure as paper records. There must be electronic safeguards to prevent external parties from

Confidentiality Outline Page 7
accessing the system. For those with legitimate access to the system, passwords (specific to the information needs of the accessor) should be used. Audit trails, which record who has accessed the records, should be monitored. For research, computer records can preserve patient anonymity better than paper records, because personally identifiable information can be “masked” more easily. Computer records also facilitate disclosing only partial records. One can select the information one wants to print, without having to worry about trying to photocopy some information from a page but not other information.

In general, security must keep up with the technology and anticipate possible breaches. The HIPAA Electronic Transaction Standards will require that health care plans, providers and clearinghouses adopt uniform security requirements. However, they also give access to sensitive information without requiring specific consent. Some commentators believe the new regulations undermine privacy rather than enhancing it.

(b) Withholding Information

If a patient asks you not to put certain information into his record, should you comply? “How much will not knowing this information compromise patient care?” is a key question relating to this decision. Suppose your patient sees another doctor in an acute situation. What will the other doctor need to know? Say a 40 year-old woman had an abortion when she was 20. It is unlikely that this information will be needed for her care. On the other hand, withholding information about the medications she is currently taking could have serious repercussions.

It seems appropriate to defer to patients’ wishes when the risk of harm to the patient or others is small. Assessing this risk will often be difficult.

(c) HIV/AIDS

HIV/AIDS has increased interest in patient confidentiality. It raises difficult issues because patients with HIV/AIDS are especially vulnerable to harms caused by disclosure. On the other hand, HIV is communicable, and we want to protect others from catching it. Sometimes disclosing information can help in this effort. Widespread breaches in confidentiality, however, would not only harm the patients, but they would be bad for public health as they would discourage others from being tested and treated.

The HIV/AIDS Information Center writes that confidentiality is part of an effective response to the disease. State funded Counseling, Testing, Referral, and Partner Notification (CTRPN) sites can provide HIV tests that are not only confidential, but also anonymous. Other physicians’ tests are confidential, but
not anonymous. They include names, and are reported to the Department of Health. Anonymous tests do not include the patient’s name.

The following cases illustrate the tension between respecting one person’s privacy and harming another. Sometimes one can be tested for HIV without consent, and the results disclosed to others. In Nebraska, a person who has been convicted of sexual assault can be required to take an HIV test. The results are shared with the criminal, the victim, the court, and the Department of Health. When an emergency service provider is significantly exposed to a patient’s blood, she can petition the court to order an HIV test, and disclose the results. In this situation, if a blood sample is already available no court order is needed for testing. Testing an infant for HIV can reveal the HIV status of the mother. An infant who tests positive may or may not actually be infected, but her mother definitely is. Breast-feeding is likely to infect the infant. So, it is in the infant’s best interest for her mother to know her own HIV status (so that she does not breast-feed), yet this information may be obtained without the mother’s consent.