Legal Issues...Maintaining Confidentiality: an Overview

Issue Description
This article will discuss confidentiality of patient information. Physicians have maintained the confidentiality of patients’ personal medical information for thousands of years.(1) The ancient Hippocratic oath mandates confidentiality as an essential element of ethical treatment of patients. Patients would be reluctant to disclose private information to physicians if they thought it may become public knowledge. Consequently, patients’ health could be endangered if physicians were unable to make correct diagnoses due to incomplete or wrong information.(2) Before the advent of the digital age it was easy for physicians to maintain confidentiality of patients’ medical information – they did not discuss the information with anyone not authorized to receive it, and they kept patient paper records secure in locked filing cabinets. In the pre-digital age and, to a certain extent now, privacy of information is protected by inefficiency and “general chaos” but at a high cost of health care quality .(3) However, health care providers in the United States are now required to use electronic storage. This increases availability of medical information during emergencies, increases continuity of care when a patient receives care at a facility remote from the location of their medical records, reduces prescribing and other errors, reduces wastage of resources(4) and, finally, facilitates research on health measures and outcomes.(5) It appears that in Germany and Japan centralized databases already store patient information on behalf of health care providers.(6) However, people differ widely in their views on electronic versus paper records – the disadvantage of electronic storage and conveyance is that privacy of information is endangered. Therefore, more attention than ever before is being paid to the issue of confidentiality. How do we achieve the admirable aims described above and at the same time prevent unauthorized access or even theft of personal medical information?(7) The problem now is that the consequences of leakage of medical information are much more severe. Previously, unauthorized disclosure of paper records was limited in extent. On the other hand, electronically stored information that is leaked can be disseminated on the Internet to an unlimited extent. Moreover hackers have deleted information and held hospitals to ransom.

Another issue raised is whether a physician should retain certain kinds of health records indefinitely. An example given is that of a student who had a battery of tests for sexually transmitted infections after an encounter with a commercial sex worker. The tests results were negative. This indiscretion was never repeated. Should the negative results be kept by the student’s physician indefinitely?(8) The suggested answer is that physicians should retain records that may reasonably be of value to the patient. Or, phrased another way, would another physician need those records when evaluating the patient for the first time?(9) Research conducted during clinical trials yields private information about patients. People participating in clinical trials often do not understand the contents of the written informed consents that they sign and they usually do not read them anyway. One solution is “opt out” where patients are given the choice of preventing all or part of their medical data being revealed.(52) Another solution involves the Federal Drug Administration (FDA) developing guidelines for so-called “moderated asymmetric confidentiality” under which private information may be disclosed only to the FDA.(50)
Social media on the internet, in particular Facebook, present a problem of confidentiality if personal medical information is posted. Health care workers must be careful not to inadvertently post such information about patients. On one occasion a nursing student posted inappropriate information on her MySpace page about her experiences in witnessing the birth of a baby. Her expulsion from her nursing school was reversed by the court. See also, Recommendations, below.

A proposed federal rule was published on May 31, 2011 requiring the disclosure to patients of the identity of organizations and individuals that access their health records maintained by third parties such as hospitals. Hospital industry associations oppose the rule as placing too much of a burden on health care providers compared to the benefit it will provide to patients. In their turn, hospitals are responsible under the federal Health Insurance Portability and Accountability Act (HIPAA) Omnibus Final Rule for the unlawful disclosure of private health information by their contractors and they should take suitable steps to mitigate the attendant risks. Such steps include technical, physical, and administrative safeguards when using outside IT services (“the cloud”). Individual nurses should read their organization’s acceptable use policy before using its equipment for personal business. Your computer game might disrupt the hospital’s IT network or introduce malware.

A federal regulation, effective January 10, 2011, prohibits employers with at least 15 employees from obtaining genetic information (family medical history or genetic tests) about employees or prospective employees. If an employee casually discloses family medical history the employer may not request further genetic information (the “water cooler” problem).

In Australia the Privacy Act, 1988 was amended and a mandatory privacy guideline was promulgated under the statute severely restricting the dissemination of genetic information.

Definitions
The first four definitions are taken from the Report by the National Committee on Vital and Health Statistics, June 22, 2006.

The Committee’s definition of “privacy” for the purpose of health information is narrower than its common or constitutional law meanings.

› Privacy: In relation to health information, “privacy” is defined as an individual’s right to control the acquisition, uses, or disclosures of his or her identifiable health data.

› Confidentiality: The obligations of those who receive information to respect the privacy interests of those to whom the data relate. In these definitions, “privacy” refers to a patient’s rights while “confidentiality” refers to a caregiver’s obligation to respect those rights.

› Security: The physical, technological, or administrative safeguards or tools used to protect identifiable health data from unwarranted access or disclosure.

› Nationwide Health Information Network: The proposed nationwide electronic network of health information relating to all individuals and others that will be available to authorized caregivers but will be subject to controls that will prevent unauthorized access.

› Preemption: Under the Supremacy Clause of the US Constitution (Article VI, Clause 2), the law of the US (federal law) is the supreme law of the land despite any State laws to the contrary. This is called “preemption”. Sometimes preemption is expressly provided for in a particular federal law and at other times preemption is implied. If a State law directly conflicts with a federal law and cannot be reconciled with it, then preemption is implied. Also, if a federal regulatory scheme is so pervasive that it “occupies the field” in that area of the law, an inference can be drawn that Congress did not intend the States to supplement it and the State law is preempted.

Risks
The National Committee on Vital and Health Statistics emphasized in its Report that the electronic Nationwide Health Information Network that it advocated, entailed increasing risk to the privacy and confidentiality of private medical information. However, allowing individuals to control what information can be used increases flexibility but results in excessive costs and greater complexity Therefore, a compromise should be reached. The Committee describes recommended methods of balancing the need for medical information with the individual’s desire to control access to personal medical information. It has been suggested that certain types of sensitive medical information should receive special protection, for example, mental health and substance abuse. However, HIPAA only makes special provision for psychotherapy notes.

Although health care providers do not need patients’ consent to record their private information electronically, this is not the case with dissemination of the same information to others such as a regional health information organization or medical record bank. There are also other ways in which the privacy of electronic patient information can be compromised – information
published on social networking Web sites pose new risks for physicians who must guard against situations that compromise private patient information. The Substance Abuse and Mental Health Services Administration announced that researchers were not bound by the confidentiality regulations in 37 Code of Federal Regulations Part 2, which requires that each patient must individually give consent before their information is released. However, this can harm people with substance use disorders. Attempted loosening of substance use disorder patient confidentiality occurred with the proposal of the Overdose Prevention and Patient Safety Act (H.R. 3545) in 2017 and a bill to amend the Public Health Service Act (S.1850).

In the view of the United States Centers for Disease Control and Prevention (CDC) the dissemination of health information under certain conditions is not necessarily to be avoided because this can promote the work of state and local programs for the prevention of sexually transmitted diseases and tuberculosis. Therefore, sharing of some public health information can constitute a public health benefit.

Extra measures should be taken for high risk electronic health information, whether by reason of the identity of the patient or the nature of the illness. For example, top hospitals in Los Angeles have, to their cost, suffered breaches of security in celebrities’ medical records, sometimes even for mundane maladies. Also, mental health, substance abuse, chemical dependency, and HIV/AIDS records require a higher level of security.

There are limits to the confidentiality rules for health care workers. For example, in the US physicians and nurses are obliged to report all suspected physical abuse to Child Protective Services. Failure to report carries serious consequences for the doctor or nurse. Also in California, physicians are obliged to report to the Department of Motor Vehicles (DMV) (via the local health officer) any medical disorder of their patients characterized by lapses of consciousness, or any other disorder that will serve public interest. The DMV holds an administrative hearing at which the patient is entitled to legal representation, and the hearing officer may restrict, suspend, or even cancel the driver’s license. Mandatory reporting laws also extend to various other situations such as reporting communicable diseases, protecting an assault victim from further harm, protecting the public from violent criminals, and assisting law enforcement in solving crimes. In these situations the “preemption” rule will not apply (see Definitions above) and HIPAA provisions takes a back seat to State laws.

In 2015 large quantities of confidential patient data possessed by Anthem, Inc., a large health insurer based in Indianapolis, were stolen by hackers, probably from China. All insured US patients now have to confront the possibility that their patient data may be hacked and stolen at any time.

**Units Potentially Involved**

**Emergency Department:** Health care professionals working in emergency departments encounter problems relating to confidential patient information that are unique to the emergency department. Overcrowding places a strain on privacy even if movable privacy screens are employed. Visitors should be allowed only with the patient’s permission, but the presence of law enforcement officers may sometimes be necessary or desirable. Sometimes higher duties conflict with the duty to keep patients’ private information confidential. These higher duties include the duty to treat patients efficiently and according to the applicable standard of care, to protect third parties, and to obey the law (see above).

**Medical Offices:** If a thief breaks into a medical office or clinic and steals patient records, who is liable? The doctor is not liable for breach of confidentiality because the records were not voluntarily given to the thief. The thief would be liable for the crimes of breaking and entering, and burglary, and would also be civilly (but not criminally) liable for invasion of privacy. This situation occurred during the Watergate episode when men (the “plumbers”) were hired by the White House to steal Daniel Ellsberg’s psychiatric records from his psychiatrist, Dr. Lewis Fielding.

**Pharmacies:** The privacy problem is especially acute in retail pharmacies where customers purchase medications for treatment of mental health issues. Suggested solutions were dispensing in plain packaging, pharmacists being more discreet in asking questions, and allocating private areas for consultations. However, dedicated consultation areas in pharmacies have been unsuccessful in the UK because these areas were also used for other purposes and were not patient friendly. Chaplain’s Offices: Some churches own and operate hospitals employing chaplains to care for the religious and spiritual needs of patients and their families. Most, if not all, hospitals permit independent chaplains to visit patients for the same purpose. What is the ethical and legal position of these chaplains when they learn confidential medical information about patients? From an ethical standpoint some chaplaincy organizations subscribe to a code of conduct for their members. Confidentiality issues under HIPAA may depend on whether the chaplain is employed by the hospital or is independent. If employed by the hospital it
has been argued that the chaplain can obtain access to confidential medical information as part of the health care team.\(^{56}\) In that situation the chaplain is bound by HIPAA confidentiality rules as are other members of the health care team. The chaplain would remain bound by HIPAA confidentiality after gaining the same information from other sources. It has been argued that “chaplains are not privy to the biomedical particulars of their case [medical records] and that biomedical professionals are not privy to what patients confide to a chaplain.”\(^{22}\)

**Court Cases and Statutes**

Although there is no reference to a right of privacy in the US Constitution, two influential lawyers, Samuel D. Warren and Louis D. Brandeis suggested in 1890 in the *Harvard Law Review* that a fundamental right of privacy is inherent in the US Constitution. This was eventually recognized by the US Supreme Court seventy-five years later in the case of *Griswold v Connecticut*. A Connecticut state law prohibited the use of contraceptives was struck down by the Court on the grounds that it violated the constitutional right to marital privacy.

In 1990 the case of *Cruzan v Director of Missouri Department of Health*\(^{29}\) went on appeal to the US Supreme Court after Nancy Cruzan suffered severe brain damage in a car accident. She fell into a persistent vegetative state and was under the care of a hospital administered by the Missouri Department of Health. Hospital physicians inserted a feeding tube that kept her alive. Her family wanted to withdraw life support but the hospital refused. The US Supreme Court held, after she had been on the feeding tube in a coma for seven years, that only Nancy had the right under the Due Process Clause of the Fifth and Fourteenth Amendments of the US Constitution to elect to withdraw life support. However, she was in a coma and could not communicate her wishes. Since the family had not introduced “clear and convincing” evidence that Nancy would have wanted life support withdrawn the Court held that the family could not compel this. The family went back and introduced clear and convincing evidence that she would have wanted life support withdrawn. They eventually won a court order that life support be terminated and Nancy died eleven days later. This case indicated that the right to regulate one’s own medical treatment is regarded as a privacy right protected by the liberty interest of the Fourteenth Amendment.\(^{30}\)

The Oregon case of *Humphers v First Interstate Bank of Oregon*\(^{31}\) involved a woman who gave birth to a daughter whom she gave up for adoption. Her hospital records were sealed. The mother eventually married and only her physician, husband, and mother knew about the adoption. Twenty-one years later the daughter, Dawn, wanted to find out about her origins. She enlisted the help of her biological mother’s physician at the birth. The doctor gave Dawn a letter falsely stating that he had administered diethylstilbestrol to the birth mother and the possible consequences of this made it important for Dawn to contact her birth mother. There is no indication whether or not Dawn knew that this statement was false. Relying on this letter, the hospital allowed Dawn to copy the medical records, which enabled her to contact her birth mother, Ramona. The contact upset Ramona and caused her emotional distress, sleeplessness, humiliation, embarrassment and inability to function normally. In the meantime, the doctor had died. Ramona sued the physician’s estate on five claims including breach of a confidential relationship and invasion of privacy (the other grounds were “outrageous conduct”, conduct below the standard of care, and breach of contractual obligation of secrecy). The trial court dismissed all five claims on defendant’s pretrial motion to dismiss. The Oregon Court of Appeals reversed the trial court on the claims for breach of a confidential relationship and invasion of privacy. On further review, the Oregon Supreme Court sitting en banc (usually eleven judges), in view of the importance of the case, held that Ramona had a claim arising from the doctor’s breach of a professional duty to keep her secret rather than from a violation of her privacy. Ramona was, therefore, permitted to go to trial claiming breach of confidentiality but not invasion of privacy. The Supreme Court emphasized that although these claims (breach of confidentiality and invasion of privacy) both assert the right to control information, they differ in important respects – only a person (for example a doctor) who holds information in confidence can be charged with a breach of confidence. On the other hand, an unlawful invasion of privacy can be committed by anyone. (The term “privacy” is used here in a general sense and not in the restricted sense set forth in the Definitions, above.) The Oregon Supreme Court also held that this was not a situation where the doctor had a duty to disclose the information. Nor was it a situation where Dawn, the daughter, needed the information for medical reasons, as the doctor pretended. In those situations the disclosure of private information would likely have been privileged and not subject to liability. Finally, the Court noted that Oregon statutes mandate the secrecy of adoption records.

The issue of patient confidentiality arose in an interesting context in 2008 in an Oklahoma City, Oklahoma case when an African-American nurse aide, 49, was disciplined for alleged errors in patient charting. She filed formal accusations of discrimination with the US Equal Employment Opportunity Commission (EEOC). To support her case she copied other patients’ charts to show that other nurse aides, younger and non-minorities, had made the same charting errors but were not disciplined. She was then kept on staff for more than a year before management discovered that she had copied unredacted materials from other charts. They then reported her to the Oklahoma Department of Health and terminated her.
The state Department of Health conducted an independent investigation and found that she was guilty of patient abuse by misappropriating personal property belonging to a resident – the information in the charts was regarded as residents’ personal property. The aide sued the nursing home in federal court for retaliation but not for discrimination. This was different from her EEOC claim in which she complained of discrimination. The Tenth Circuit US Court of Appeals (covering Oklahoma) held that retaliation is not permitted after a claim is filed with the EEOC. However, management did not retaliate against her. They terminated her for violating patient confidentiality and not as retaliation for her EEOC complaint. Her claim was, therefore, dismissed by the appeal court. \(^{(32)}\)

A charge nurse at an Oregon nursing home had a long history of personnel disputes and disciplinary issues with her employers concerning the quality of her care and patient charting. She photocopied and took home her own and other nurses’ patient charts to allegedly protect herself if she was reported to the state board of nursing. She was terminated and she sued for wrongful discharge and other claims. The US district court held that she was permitted, in her supervisory capacity, to copy patient records made by nurses under her supervision and forward them to the administration of the nursing home as part of evaluations of their performance, as long as the records remained at the facility. However, a nurse may not copy patients’ records for her own self-protection. She made the violation worse by taking the copies home. Also, identifying information must be redacted from patient records if the records are used in a court case not involving the patient. \(^{(33)}\)

Federal and New York law permit the release of mental health records without the consent of the patient as long as a prior court order is obtained authorizing the release. A prisoner, Leroy Dorsey, incarcerated in Sing Sing Correctional Facility, filed a habeas corpus petition for his release and he contended that his claim for release was not out of time due to his mental condition. The court ordered that the Kings County district attorney’s office produce any documentation relevant to Dorsey’s claim about his mental condition. The Attorney General’s office then applied for and obtained an order to release Dorsey’s psychiatric records from Sing Sing. Dorsey then filed a claim against the New York State Office of Mental Health and others saying that it had improperly disclosed his private medical records containing confidential HIV-related information without his written permission. The court held that Dorsey did not allege in his claim that information concerning his HIV status, testing or exposure was disclosed. He only alleged that the records may have contained such information. Since there was no allegation of disclosure, the court dismissed the claim.

A Louisiana lawsuit illustrates a hospital’s confusion as to when private medical information should be revealed to police authorities. A woman was battered by her husband and admitted to the hospital. A nurse called the Lafayette police to report the attack but the hospital case manager, citing HIPAA, would not let them speak with the victim. The case manager was unmoved when a senior police officer explained to her that a Louisiana statute required the investigation and that the hospital was obliged to cooperate. The case manager was then arrested on a charge of obstruction of justice but the charges were later dropped by the prosecutor. The case manager later sued the police department for violation of her civil rights alleging that the police should have known her refusal was justified by HIPAA confidentiality provisions. The court disagreed, holding that HIPAA permits the police to obtain information of a crime directly from patients and the police had probable cause to arrest her for obstruction of justice. A commentary on the case states that a failure to understand HIPAA carries serious implications for victims of violent crime and that hospitals should be familiar with state laws concerning police investigation. \(^{(34)}\) A feature of the case report is that no mention is made as to whether the hospital requested the victim’s permission to allow the police to interview her for the purpose of investigating the attack against her.

The US Supreme Court case of Sorrell v IMS Health, Inc. \(^{(35)}\) held that a Vermont statute prohibiting the sale by pharmacies of prescription information acquired from physicians, and prohibiting its use for drug sale promotion, unconstitutionally restricted the free speech rights of drug manufacturers. Although patients’ names were not part of the information sold, names could be extracted from the information. \(^{(36)}\)

The Health Insurance Portability and Accountability Act (HIPAA) was enacted by Congress in 1996 in reaction to the increasing popularity of the electronic transfer of medical information. However, compliance became mandatory for most entities only in 2003. \(^{(37)}\) The Office for Civil Rights (OCR) is the section of the Department of Health and Human Services responsible for enforcing the HIPAA privacy rule. Up to March 2007, the OCR had received about 26,000 complaints from the public that the confidentiality of their medical records had been violated. Many of these were settled by the OCR through mediation but no civil monetary penalties have been enforced. The Department of Justice has prosecuted only a few criminal cases for violations of the HIPAA privacy rule. More enforcement is necessary to gain the confidence of the public. \(^{(38)}\) HIPAA provides a comprehensive national standard for the privacy of health information whereas previously the states each had their own laws, if any. The Privacy Rule and the Security Rule under the Act are summarized on the internet at the Department of Health and Human Services website. \(^{(39)}\) Civil penalties of $100 per negligent violation can be levied...
while criminal penalties are reserved for those who knowingly obtain or disclose personal patient information.\textsuperscript{(40)} The regulations under the Act apply to all US practitioners and health care institutions that electronically transmit “protected health information” as defined in the Act. The key elements of the definition are health information (including information about provision of care or payment for care) in any medium that is identifiable with a particular individual\textsuperscript{(41)} even after death.\textsuperscript{(42)}

An investigation of state laws in 2013 relating to dissemination of private medical information by state and local authorities indicated that they differ to a certain extent from each other.\textsuperscript{(42)} Personal medical information held by public health agencies is not protected by HIPAA.\textsuperscript{(62)} Only state law is available to protect it. Twenty five states have no presumption of privacy of public health information. Other states have such a presumption with certain exceptions.\textsuperscript{(43)} This diversity of regulation presents problems for public health initiatives.\textsuperscript{(51)} Therefore, public health organizations have attempted to remove identifying material from their information to improve confidentiality – a process called “de-identification”. Health information without any personal identifying material is generally legal and acceptable under HIPAA. However, courts will not forbid the disclosure of public health information in the absence of clear proof that re-identification of individuals is possible.\textsuperscript{(51)}

In 2015 a registered nurse in the UK, employed as an occupational health adviser with the National Health Service, was suspended for 18 months by the Nursing & Midwifery Council for endangering the confidentiality of patient information. He had an unencrypted memory stick in a computer containing identifiable clinical information and also sent unencrypted e-mails containing this information to himself and a colleague.\textsuperscript{(54\textendash}60)}

In the European Union disclosure of personal medical information is subject to a strong regulatory regime. Processing operations for the collection of this information must be cleared by the European Data Protection Supervisor before they are implemented. Processing operations include pre-employment medical examinations, medical checks, and research projects. Individuals enjoy legally enforceable rights to be informed about collection of their information and to stop such collection in most circumstances.\textsuperscript{(44)} The new European Union General Data Protection Regulation, in force from May 2018, will also affect UK businesses and healthcare institutions and their data centers outside Europe or the UK. Stringent protections will apply; for example, businesses must identify what data was affected within 72 hours of a data breach.\textsuperscript{(65)}

**Recommendations**

The National Committee on Vital and Health Statistics recommended in 2006 that individuals should not be compelled by their health providers to have their personal medical information electronically recorded.\textsuperscript{(5)} Even if they consent to this, they may block access to specific content. Individuals are often compelled to grant access to their health records as a condition of applying for jobs, insurance policies or loans.\textsuperscript{(45)} The universal electronic health records system should not permit disclosure of information not pertinent to the enquirer’s purpose. For example, a life insurance company will only be able to access information relevant to mortality risk. The Committee terms this “contextual access criteria.” To avoid circumvention of this restriction, insurance companies and others should be compelled to include an express restriction in the releases that their customers sign. HIPAA and some state laws impose restrictions on the dissemination of private medical information. Universal electronic access to this information may conflict with some provisions of these laws. Therefore, the Committee recommended that the federal Department of Health and Human Services work to harmonize the new system with federal and state privacy laws.

The American Nurses Association’s Code of Ethics for Nurses with Interpretive Statements (2015) provides guidelines on the disclosure of personal medical information, including posting information on social media on the internet.\textsuperscript{(46)} The American Health Information Management Association published updated guidelines in 2011 on complying with the provisions of the federal Health Information Technology for Economic and Clinical Health Act (HITECH) and how to handle violations when they occur. Under this Act individuals must be notified when their health information is disclosed in violation of HIPAA. When a breach involves more than 500 individuals, it must also be reported to the Secretary of Health and Human Services and the media. Violations must be consistently sanctioned by the institution however senior the violator may be in the organization. Sanctions may differ for accidental violations, failure to follow organization policy, and willful violations made with harmful intent.\textsuperscript{(47)} It is recommended that institutions conduct adequate security risk assessments especially since they enable institutions to qualify for government subsidies.\textsuperscript{(48)}
References

7. Report by the National Committee on Vital and Health Statistics, supra, pp. 3-4, 12.
15. See, for example, Joel Martin Geiderman, et al, supra, at p. 636 et seq.
17. Mark A. Rothstein, supra, at p. 494.
27. Joel Martin Geiderman et al, supra, at p. 637.
34. 131 S Ct. 2653 (2011).
37. Mark A. Rothstein, supra, at p. 500.
40. Joel Martin Geiderman et al, supra, at p. 638.
44. Mark A. Rothstein, supra, at p. 496.


