IOM, For the Record, "Systematic Concerns About Health Information", pps. 65-81, 1997

1. As noted by IOM (1997), systemic concerns about the privacy of patient-specific health information are generally rooted in the use of such information in a manner that acts against the interests of the individual patient involved. Specific identifiable adverse consequences of disclosure may include:
    a. Increased difficulty in obtaining employment or promotion
    b. Increased difficulty in obtaining health or life insurance
    c. Personal embarrassment or discomfort
    d. All of the above

2. The financial services industry was able to encourage consumer adoption of credit card usage by assuaging consumer fears of identity theft by offering consumers, in the event of credit card loss or identify theft, financial compensation and/or limiting consumer financial exposure to harm. Such potential harms to credit card customers were arguably financially quantifiable. With respect to potential harms to patients arising from unauthorized personal health information disclosure, which of the following harms is arguably the most difficult to financially quantify:
    a. Increased difficulty in obtaining employment or promotion
    b. Increased difficulty in obtaining health or life insurance
    c. Personal embarrassment or discomfort

3. As noted by IOM (1997), an individual's health information is of use to both "primary" and "secondary" users. Which of the following is <u>not</u> considered a "primary" user:
    a. Primary care provider
    b. Specialist consulted by primary care provider
    c. Emergency care clinic
    d. Long term care facility
    e. Health insurance payor

4. Which of the following is <u>not</u> considered a "secondary" user:
    a. Medical researcher
    b. Clinical laboratory
    c. Social welfare agency
    d. Pharmaceutical company
    e. Medicare

5. In the Health Insurance Portability and Accountability Act (HIPAA) of 1996, Congress mandated the Secretary of Health and Human Services to promulgate a standard for a Universal Patient Identifier. The IOM (1997) noted that a universal identifier will facilitate the linking of information across data sets, which could be
    a. Desirable in making individual patient medical records more complete for optimal health care

b. Desirable for making unusual patterns of healthcare usage and potential fraud discoverable
c. Undesirable in making an individual's health data more accessible to linkage with personal financial and other data, increasing the prospects for discrimination and loss of privacy
d. All of the above

NAHDO, "All-Payer Claims Databases: an Overview for Policymakers", 2010, 11 pps

Starr, Paul, "Health and the Right to Privacy", 25 Am. J. of L. & Medicine 193 (1999)

6. As noted by Paul Starr (1999), privacy is
    a. An absolute Constitutional right that trumps all other societal interests in a particular health data record
    b. An absolute Constitutional right that trumps all other societal interests in a particular health data record, except in cases of national security
    c. A non-exclusive Constitutional right that can be subordinated to society's needs only in cases of government-operated public health services needs
    d. A non-exclusive Constitutional right that can be judiciously balanced against society's various interests and data needs, including medical research and law enforcement

7. In Paul Starr's opinion (1999), a prohibition on outright merchandising of any health data for purposes unrelated to those for which patients provided the original information
    a. Is a necessary consequence of a person's right of privacy
    b. Is a necessary consequence of a health provider's ethical obligations
    c. Would be unfortunate in prohibiting some useful efforts in disease management, as the net benefits of such a policy may not be substantial
    d. Should be modified to allow patients to receive monetary compensation from the commercial utilization of their data

8. As noted by Paul Starr (1999), the collection of patient consents for "secondary" use in medical research of clinical data
    a. Raises the cost of conducting desirable research, particularly for large epidemiological studies
    b. Results in incomplete or selective data sets, fatally impairing the validity of the study
    c. Reflects reliance on a "misplaced individualism" to rest the burden of protecting privacy on the individual data subject rather than on the institutional data user
    d. All of the above

9. In Paul Starr's opinion (1999), the adoption of a federal government individual patient universal health identifier
    a. Is undesirable as the first step down the slippery slope of totalitarianism

b. Is unnecessary, as other identifiers exist for most adult U.S. citizens
c. Can be delegated for implementation to the IRS
d. Can assist in the conduct of medical research by making it easier to anonymize data in research

10. As noted by Paul Starr (1999), the concept that a federal privacy law should preempt all state privacy laws
    a. According to privacy advocates would reduce privacy protection in certain states whose privacy laws are more stringent than the federal law
    b. According to the healthcare industry would be desirable to simplify the legal requirements with which it must comply and create a consistent national framework
    c. Would reduce the role of the States as "laboratories of democracy" in which new approaches to privacy protection could be tested
    d. All of the above

Rodwin, Marc A., "The Case for Public Ownership of Patient Data", 302 JAMA 86-88 (2009)

11. Marc Rodwin (2009) suggest that society has an ownership interest in individual patient health data because
    a. The data was generated with the financial assistance of other patients and the general public through fees, insurance payments and taxes
    b. The societal benefits from forming comprehensive databases required for medical research and innovation outweigh the claims of ownership of institutional custodians of data
    c. The data was collected by medical professionals whose core ethical values are to promote patients' interests, medical knowledge, and public health
    d. All of the above

12. Marc Rodwin (2009) suggest that there should be no private ownership of individual patient health data because
    a. In seeking healthcare treatment which is subsidized and made possible by the government, the individual benefits from a publicly-enabled service and implicitly accepts that data resulting from the service are the property of the government
    b. Healthcare data is collected and created collectively by multiple healthcare providers, requiring multiple diagnostic equipment and skills, favoring collective ownership rights
    c. The economic benefits that usually support private over public ownership do not exist for health data since private ownership is unnecessary to ensure the production of individual patient health data, and would preclude downstream inventions and benefits for individual owners and society
    d. None of the above

Fair Information Practice Principles

13. The Fair Information Practice Principles do not:
    a. Specify whether implied consumer consent (opt-out) is a satisfactory method for satisfying the principle of Individual Participation
    b. Specify what, if any, remedial steps a data custodian should take in response to a data privacy breach
    c. Specify whether a broad description of potential future uses of personally identifiable data is a satisfactory method for satisfying the principle of Purpose Specification
    d. Specify whether patient consent needs to be limited in duration
    e. All of the above

NCVHS, "Health Data Stewardship: What, Why, Who, How – An NCVHS Primer", 2009

14. Under the NCVHS concept of "data stewardship" (2009), who has data stewardship responsibilities:
    a. Only licensed healthcare providers
    b. Only HIPAA "covered entities"
    c. Only the party creating data in a data set
    d. Every organization that handles health data

15. Which of the following rights of individual patients are not within the scope of NCVHS "data stewardship" (2009):
    a. Access to the individual's health data
    b. Consent of the individual for use of the individual's data
    c. Referral of provider charges which are contested by a patient to a government ombudsman for review
    d. Opportunity of individual to correct one's own health data

16. Public comments received in response to a 2004 proposal of the U.S. Agency for Health Research and Quality (AHRQ) for the creation of "national health data stewardship entity" (NHDSE) reflected
    a. A preponderance of support for the creation of an NHDSE
    b. A preponderance of opposition to the creation of an NHDSE
    c. A relatively even split between those favoring and opposing the idea

17. Under the NCVHS concept of "data stewardship" (2009), patient consent for the use of data
    a. Must be evidenced by a signed writing, witnessed and notarized
    b. Is absolute; the individual's choice is not subject to waiver or disregard by any person, regardless of the intended use of the data
    c. May vary in degree depending on the type of information, the purpose of the data sharing and governmental population health needs

Center for Democracy & Technology, "Rethinking the Role of Consent in Protecting Health Information Privacy" (Jan. 2009)

18. The HIPAA Privacy Rule as initially proposed by HHS (Dec. 28, 2000) required the collection of patient consent for most routine uses and disclosures of the patient's protected health information (PHI). The Privacy Rule was subsequently revised (Aug. 14, 2002) to provide:
    a. Patient consent is not required for use and disclosure of PHI for purposes of "treatment", "payment" and "healthcare operations"
    b. Patient consent is not required for any purpose desired by a licensed healthcare professional or facility
    c. Patient consent is not required for any purpose desired by a licensed health plan or health insurance company
    d. Patient consent is not required if the patient is enrolled in Medicare
    e. Patient consent is not required if the patient is a registered owner of a firearm

19. The Center for Democracy & Technology (CDT) in 2009 was of the view that the final version of the Privacy Rule then in force
    a. Strikes the right balance between the needs of the healthcare system for health data to flow for a variety of health-related purposes, and the rights of patients to exercise some control over data utilization for non-health purposes through patient authorization
    b. Inadequately protects patients' rights and should be revised to require patient consent for all uses and disclosures of PHI
    c. Excessively restricts the ability to collect and analyze "big data" and the conduct of medical research
    d. Excessively restricts healthcare facilities from using PHI for marketing and fundraising purposes
    e. Excessively restricts the acquisition and use of electronic health record (EHR) systems

20. The Center for Democracy & Technology (CDT) in 2009 was of the view that the "core health care functions" for which patient PHI should be shared without collecting patient consent should specifically <u>not</u> include:
    a. Behavioral health and substance abuse counseling in outpatient and ambulatory facilities
    b. Assistance of social worker in securing housing for the patient
    c. A health information exchange (HIE)
    d. None of the above; the CDT did not specify the components of "core health care functions"

21. For enabling electronic health information exchange among providers, at the HIE network level the CDT in 2009
    a. Favored centralized patient data storage to relieve small healthcare services providers of the implementation burden of increasing technical requirements of data security

b. Favored centralized patient data storage to reduce data transmission latency between the data custodian and the data requestor
c. Favored centralized patient data storage to facilitate medical research;
d. Opposed centralized patient data storage as being more vulnerable to breaches

22. The Center for Democracy & Technology (CDT) in 2009 was of the view that requiring patient prior consent for nearly every use of health information would not have provided meaningful privacy protection because:
    a. If providers could refuse to treat persons who withheld consent, the patient's right to consent would be illusory as there would have been no meaningful right to withhold consent;
    b. Providers would use broad blanket consents to avoid unnecessarily hampering the provision of payment for health care
    c. Both of the above
    d. None of the above

23. The Center for Democracy & Technology (CDT) in 2009 was of the view that collection of consents from patients for the use and disclosure of PHI is flawed because
    a. When consents are collected at the time of receiving healthcare services or signing up for health plan benefits, parents are not focused on their privacy interests
    b. Consent forms and privacy notices are written in language the average person cannot understand
    c. Patients wrongly assume that the existence of a "privacy policy" means that their PHI will not be shared
    d. Faced with too many consent forms, patients experience information overload and are less likely to try to understand the consent
    e. All of the above

24. The HIPAA Privacy Rule requires prior patient authorization to use PHI for marketing purposes, with certain exceptions. The Center for Democracy & Technology (CDT) in 2009 was of the view that
    a. Healthcare providers in their professional judgment should be free to decide which communications are beneficial to a patient's health;
    b. Patients should register their desire not to receive product and services solicitations from healthcare providers in a federal Do-Not-Call registry
    c. The exceptions should be revised to prohibit a healthcare provider from communicating to patients any information regarding a third party's products and services without prior patient consent
    d. All marketing communications should be approved by a healthcare provider's Institutional Review Board

25. The HIPAA Privacy Rule permits PHI to be used or disclosed for purposes of "healthcare operations" without prior patient consent. The Center for Democracy & Technology (CDT) in 2009 was of the view that
    a. The definition of "healthcare operations" should be revised to remove from it purposes which are not necessary to facilitate "core" treatment and payment functions
    b. The PHI data to be used or disclosed for "healthcare operations" should be first scrubbed of common patient identifiers, depending on the specific need for such personally identifiable information
    c. Both of the above
    d. None of the above

26. Regarding the electronic exchange of PHI data through a Health Information Exchange (HIE), the Center for Democracy & Technology (CDT) in 2009 distinguished between HIEs that merely facilitate the exchange of data among covered entities, and those that collect and store data or have independent rights with respect to the data. The CDT suggested that
    a. The different HIE architectures raise different privacy and security risks
    b. The distributed PHI database network architecture better maintains the local data custodian's responsibility for compliance with local laws and patient privacy rights
    c. An HIE's ability to electronically aggregate patient data raises the possibility that the HIE may look at tertiary uses of patient PHI data to generate income
    d. All of the above

27. Regarding the storage of PHI in a Personal Health Record (PHR) under the patient's control, the Center for Democracy & Technology (CDT) in 2009 was of the view that
    a. IT companies offering Internet-based PHR products or services, such as Microsoft, are not "covered entities" subject to the HIPAA Privacy Rule
    b. Consumer consent should be required for any person to access or disclose PHI in a PHR
    c. In addition to HHS enforcement of the HIPAA Privacy Rule, patients as consumers should have their privacy rights addressed by FTC regulation of PHRs
    d. All of the above

McDermott, Will & Emery, "The New Normal: Big Data Comes of Age", Special Report, May 12, 2104

28. The Consumer Privacy Bill of Rights is
    a. Part of the U.S. Constitution
    b. Part of the 2010 Patient Protection and Affordable Care Act
    c. A regulation issued by the Department of Health and Human Services
    d. An Obama administration proposal that has not yet been enacted into law

29. The Consumer Privacy Bill of Rights is founded upon
    a. The Triple Aim

b. Fair Information Practices Principles
c. Meaningful Use
d. Payment Card Industry Data Security Standard (PCI DSS)

30. As reflected in its "Big Data" report (May 1, 2014), the Obama administration
    a. Favors enactment of the EU model into U.S. federal law
    b. Favors enactment of the EU model as a multi-national United Nations Convention
    c. Favors a sectoral approach that focuses on regulating specific risks of privacy harm in particular context, such as health care and credit
    d. Favors imposition of the EU model on all recipients of federal grants and vendor contracts

31. A sectoral approach to data privacy protection, placing fewer broad rules on the use of data:
    a. Allows industry to be more innovative
    b. Fails to protect data from potential uses that fall between sectors
    c. Is typified by the 1996 Health Insurance Portability and Accountability Act (HIPAA)
    d. All of the above

32. A sectoral approach to data privacy protection would envision the creation within separate industries of sector-specific "codes of conduct" which would be ultimately enforced by
    a. The Department of Healthcare and Human Services (HHS)
    b. The Federal Trade Commission (FTC)
    c. Both of the above
    d. None of the above

33. "Big Data" analytical tools enable the discovery of correlations within large data sets. A policy to optimize the functioning of "big data" analytical tools would
    a. Discourage the collection of data to reduce the quantity of irrelevant data
    b. Encourage the collection and free flow of data to harness its power and to drive innovation
    c. Promote de-identification of data
    d. Oppose de-identification of data

34. The White House "Big Data" report (May 1, 2014) notes that the notice and consent model forms the basis of much of the current privacy and security compliance framework. In the context of "big data", however, this model may be inadequate because
    a. Notices and consents cannot be sufficiently specific to identify all future uses of the subject data
    b. The volume of required notices and consents would overwhelm the average consumer
    c. Consumers enjoy no real opportunity to negotiate consent or decline the services giving rise to the data
    d. All of the above

35. The PCAST "Big Data" report (May 1, 2014) proposes for "big data" privacy protection in place of a notice-and-consent model
    a. A system in which the entire burden of privacy protection rests with governmental authorities as trusted third parties
    b. A system in which the entire burden of privacy protection rests with data custodians
    c. A system in which the entire burden of privacy protection is shared among (i) trusted third parties that formulate various "privacy profiles", (ii) individual consumers who express their privacy preferences by selecting a "privacy profile" to govern the uses of their data, and (iii) data custodians who agree to apply the use and disclosure limitations of a particular "privacy profile" chosen to apply to the subject data
    d. None of the above

36. The White House /PCAST "Big Data" report (May 1, 2014) notes that "de-identification" and "anonymization" of data records
    a. Must continue unchanged as a cornerstone of privacy protection of all data, including "big data"
    b. Should be applied by default to all data record disclosures
    c. May be impossible in the era of "big data", requiring reconsideration of our current medical research laws and regulations
    d. Is reinforced in the era of "big data" by "data fusion"

37. In order to implement a federal uniform data security breach notification standard, the following subparts should be specified:
    a. The timeframe for notification
    b. Coordination with law enforcement to prevent impeding investigations
    c. Distinguishing among different levels of harm arising from breaches, and prioritizing among different levels of notification and mitigation responses
    d. All of the above

Goldsmith, J, "Healthcare IT's unfulfilled promise: What We've Got Here is Failure to Communicate", Futurescan 2010 pps. 32-35, 2010

38. Jeff Goldsmith (2009) notes that current electronic health record systems have failed to live up to expectations, as they are:
    a. Costly to install and maintain
    b. Not user-friendly, either with regard to clinical data capture or retrieval
    c. Lacking in payback from the investment
    d. All of the above

39. In Jeff Goldsmith's opinion (2009), the largest cost reductions in clinical care effected through health information technology will come from:
    a. Elimination of duplicate patient testing through access to complete patient charts
    b. Reduction in clinical decision errors through advanced clinical decision support (CDS)
    c. Reduction in acute care episodes through proactive patient monitoring and disease management
    d. Fully automating the revenue cycle and eliminating most of the billing staff with real-time adjudication and payment of medical claims
    e. More efficient "top-of-license" delegation of clinical tasks among clinical staff in coordinated care teams

40. In Jeff Goldsmith's opinion (2009), the optimal repository for a person's health record will be:
    a. A Personal Health Record (PHR) provided by the patient's primary care provider
    b. A Personal Health Record (PHR) provided by the Health Information Exchange (HIE) serving the patient's primary care provider
    c. A Personal Health Record (PHR) provided by an Internet-based data custodian
    d. A personal data storage device carried by or embedded within each individual