Perspectives on JAMIA Informatics

Viewpoint Paper ■

A Model for Expanded Public Health Reporting in the Context of HIPAA

Soumitra Sengupta, PhD, Neil S. Calman, MD, George Hripcsak, MD, MS

Abstract The advent of electronic medical records and health information exchange raise the possibility of expanding public health reporting to detect a broad range of clinical conditions and of monitoring the health of the public on a broad scale. Expanding public health reporting may require patient anonymity, matching records, re-identifying cases, and recording patient characteristics for localization. The privacy regulations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) provide several mechanisms for public health surveillance, including using laws and regulations, public health activities, de-identification, research waivers, and limited data sets, and in addition, surveillance may be distributed with aggregate reporting. The appropriateness of these approaches varies with the definition of what data may be included, the requirements of the minimum necessary standard, the accounting of disclosures, and the feasibility of the approach.

■ **J Am Med Inform Assoc.** 2008;15:569–574. DOI 10.1197/jamia.M2207.

Introduction

Public health departments have long required the reporting of diseases like tuberculosis that are of special public health concern.[1] The National Notifiable Diseases Surveillance System is coordinated by the Centers for Disease Control and Prevention (CDC) and relies on health care providers and laboratories to report diseases and conditions on the nationally notifiable diseases list to state and local health departments, who in turn transmit de-identified data to CDC.[2] The Morbidity and Mortality Weekly Report (MMWR) has been providing tables and trends derived from these reports since 1952.[3] The implementation of electronic laboratory information systems and vocabulary and messaging standards has led to the feasibility of electronic laboratory reporting, which can improve the timeliness and completeness of notifiable disease reporting.[4]

The expanded use of clinical information systems and the advent of health information exchange networks also make possible broader and more flexible sharing of clinical data with public health departments.[5,6] The possibility of expanding public health surveillance beyond notifiable conditions to include routine reporting of symptoms, diagnoses, procedures, laboratory data, ancillary reports, etc. may open enormous opportunities. This new-found capability could improve traditional detection and response to disease outbreaks and enable public health authorities to detect outbreaks sooner, expand case-finding, monitor the size, spread, and tempo of outbreaks once detected, quantify morbidity and impact, and monitor the efficacy of interventions. Even greater potential may be realized by expanding beyond infectious disease surveillance to a more active role for public health officials in monitoring priority public health issues such as cancer screening, adult immunizations, and screening and management of diabetes, lipid disorders and HIV.

With these heightened capabilities come special challenges of ensuring patient privacy and confidentiality.[7] The Health Insurance Portability and Accountability Act of 1996 (HIPAA) led to the generation of national health information privacy standards in the form of federal regulations,[8] which are intended to address such situations. While such privacy standards are critical, they must not prevent the sharing of information for the public good,[9] and an excellent review of the privacy regulations and their effect on traditional public health surveillance was provided by the Centers for Disease Control and Prevention.[10] However, acceptable approaches to data sharing that goes beyond traditional mandated reporting must also be defined. While recognizing that state and local privacy statutes can be more restrictive than the HIPAA privacy regulations (hereinafter referred to simply as "HIPAA"), in this paper, we review the privacy requirements of non-mandated large-scale data sharing between clinical data sources and public health, we discuss the HIPAA implications for those requirements, and we describe several approaches to accomplish expanded reporting in the context of HIPAA.

Affiliations of the authors: Department of Biomedical Informatics, Columbia University (SS, GH), New York, NY; Institute for Urban Family Health (NSC), New York, NY.

This work was supported by Centers for Disease Control and Prevention grant P01 HK000029 and National Library of Medicine grant R01 LM06910.

Correspondence: George Hripcsak, MD, MS, 622 W 168 Street, VC5, New York, NY 10032; e-mail: <hripcsak@columbia.edu>.

Received for review: 07/14/06; accepted for publication: 06/06/08.

Requirements

Scenario

Consider the following hypothetical scenario for expanded public health reporting beyond notifiable diseases and conditions. The scenario may not necessarily be feasible or desirable, but our goal is to highlight the privacy issues. A broad range of facilities including hospitals, community health centers, nursing homes, and home care agencies submit routine clinical data to a public health department electronically as soon as the data are collected. The data may be drawn from hospital stays, emergency department visits, ambulatory visits, and home visits. The data may be generated directly by health care providers, entered by other staff members, or derived from diagnostic procedures. The data may include diagnoses, procedures, laboratory results, ancillary reports, and documentation of symptoms, assessments, and plans. The health department uses the data to detect infectious syndromes, to identify surfacing health issues, and to track the quality of care administered in the region.

Patient Anonymity

Some forms of public health reporting, such as tracking the overall quality of care delivered in a region, may not require that individual patients be identified. If patient identities are not needed by the health department, then it is safest to send the department anonymized data, either by sending individual-level data that cannot be tracked to individuals, or by sending aggregated data. Assuring true patient anonymity is not trivial,[11,12] although mechanisms to distribute data that are not linkable to identities are being defined.[12,13]

Record Matching

Certain forms of surveillance and reporting require matching data that come from different entities. For example, to monitor health care quality, it may be necessary to look across institutions to tell whether proper preventive care was administered and whether some of a patient's medications interact. Diagnoses may come from a health care provider, clinical tests may come from a laboratory, and medications may come from a pharmacy benefit manager; ideally, data about the same patient should be coordinated. Therefore, although the patient need not be identified, it will be helpful to be able to correlate data about the same patient from different entities.

Re-identifying Patients

When a case is identified as being part of a cluster or potential outbreak, it may be necessary to identify the patient to confirm the case, to administer treatment, or to prevent the spread of disease. Therefore, although patient identities may not need to be attached to the data that are sent to the public health department, there may need to be a mechanism to identify the patient when it is appropriate.

Geographic Localization

Patient addresses may be important in surveillance that uses geospatial clustering. Clustering algorithms can perform better as addresses are known with finer granularity.[14] Depending on the context, zip code or street addresses may be beneficial. Detailed street addresses can be used to identify patients with publicly available information, however. Recent research has demonstrated a method for anonymizing patients' geographic location while still maintaining the ability to detect spatial clusters;[15] this may reduce the need for detailed addresses.

Temporal Localization

Certain dates, such as date of visit, can be critical in public health reporting. In fact, if real-time reporting is supported, then the date of visit may be inferred from the date of the report. For syndromic surveillance, the date of the visit is essential, and for monitoring the quality of care, the relative dates of admission and procedures may become important. Detailed dates present some risk for uncovering patient identities,[11,12] although it will be difficult to identify patients without access to care provider registration databases.

Patient Characteristics

Other patient characteristics, such as age, gender, and race, can be important in public health reporting. Whereas birth date can be used to identify a patient, age in years (or months for babies) is generally sufficient for reporting purposes but presents a much smaller risk of identification than birth date. Nevertheless, it has been shown that seemingly general characteristics like age may be combined to identify patients and that additional procedures may be necessary to achieve true anonymization.[16]

HIPAA Implications

HIPAA Mechanisms for Disclosing Health Information

The basic concept of HIPAA is that entities that provide health care and bill electronically must obtain authorization from patients before disclosing their protected health information.[10] The HIPAA provides for several exceptions to this rule. The most common exception is disclosure for treatment, payment, or health care operations, which covers most of health care providers' activities but does not cover public health reporting.

The HIPAA provides a number of other exceptions to authorization that are potentially relevant to public health reporting, and they are summarized in Table 1. Disclosures required by law such as mandated disease reporting are permitted without authorization (HIPAA Section 164.512(a)).[8] These disclosures may include patient identifiers like names, detailed addresses, and detailed dates.

Even if not specifically mandated by law, disclosures to public health authorities who are legally authorized to receive such reports are also permitted without authorization for the purpose of preventing or controlling disease, injury, or disability (HIPAA Section 164.512(b)).[8,17] Underlying legal authority to receive such reports may derive from existing state and local statutes regarding public health powers, such as responsibility to "exercise due diligence in ascertaining the existence of outbreaks or the unusual prevalences of diseases."[18,19] This mechanism allows names, detailed addresses, and detailed dates, but disclosures to public health authorities must follow HIPAA's minimum necessary standard (HIPAA Section 164.502(b)),[8] which states that the data that are disclosed must be the minimum necessary to achieve the desired goal. Providers rely on public health officials' determination that the requested data represent the minimum necessary, but the officials must still act responsibly in that determination.

Table 1 ■ HIPAA Mechanisms for Disclosing Health Information to Public Health Authorities without Patient Authorization

Mechanism of Disclosure	HIPAA Section [8]	Minimum Necessary 164.502(b)	Accounting of Disclosures	Identifiers Allowed	Address	Dates	Approach
Required by law	164.512(a)	No	Yes	All	Full	All	1
Public health activity	164.512(b)	Yes	Yes	All	Full	All	2
De-identification	164.514(b)	No	No	Code not derived from patient identifiers	3-digit zip code in most areas	Year only	3, 6
Research with IRB waiver	164.512(i)	Yes	Yes	All	Full	All	4
Limited data set	164.514(e)	Yes	No	Code that may be derived from patient identifiers (e.g., perfect one-way hash) [20]	5-digit zip code	All	5

HIPAA = Health Insurance Portability and Accountability Act.

The HIPAA allows clinical information to be disclosed if it has been de-identified, and it defines a safe harbor such that if 18 types of identifiers are removed, then the data is considered de-identified by HIPAA (HIPAA Section 164.514(b)).[8] In addition to identifiers like names, the safe harbor forbids dates more detailed than year and addresses more detailed than the first three digits of the zip code (in most areas). This renders de-identified data less useful for many public health surveillance purposes. Alternatively, a data set may be considered to be de-identified if it has been certified in consultation with a statistician.

To address the limitations of de-identified data, HIPAA defines a limited data set (HIPAA Section 164.514(e)).[8] A limited data set excludes identifiers like name, but it does allow detailed dates and five-digit zip codes. The entities involved in the disclosure must enter into a data use agreement that specifies who will receive the data and assures that data will not be further disclosed and that the recipient will not attempt to re-identify the data. The disclosure must meet the minimum necessary standard, but the limited data set definition would appear to be a good match for the minimum necessary to carry out most non-specifically mandated public health surveillance (dates and five-digit zip codes but no direct patient identifiers).

Finally, if a clinical research project includes transfer of clinical data to public health then disclosures can be made without authorization if an Institutional Review Board grants a waiver of HIPAA authorization (HIPAA Section 164.512(i)).[8] This is relevant only for a bona fide clinical study, however.

Mechanisms for Re-identifying and Matching Patients

The HIPAA includes provisions for re-identifying patients for those mechanisms set forth in Table 1 that do not include direct patient identifiers. A de-identified data set cannot contain direct patient identifiers but it may include a code maintained by the disclosing entity that can be used to re-identify a patient as long as the code is not derived from patient identifiers, it is not used for other purposes, and the code-patient mapping is not disclosed by the entity.[20] Thus, the provider's software could generate and maintain a randomly generated code unique to each patient. If a patient needed to be re-identified, for example, a public health authority could supply the provider with the code, and the provider could notify the patient or report the patient to the health authority with full identifiers as a mandatory case report.

The re-identification process can be automated. For example, if a surveillance alert is generated, then the re-identification code can be sent to the source facility electronically and adjudicated by the facility's information system, potentially generating an alert to the patient's provider or to the patient.

While the regulation states that the limited data set recipient (the public health department in this scenario) must not identify the information or contact the individual (HIPAA Section 164.514(e)),[8] it also makes it clear that re-identification is allowed by the covered entity (the data source) using a unique code (HIPAA Section 164.514(c)).[8] In this context, we interpret this to mean that if the health department chooses to use a limited data set mechanism, then it may not attempt to identify patients in the limited data set, but it may supply a re-identification code to the data source, which can re-identify the patient and take appropriate action. For example, if the health department detects a case of a reportable disease in a limited data set, it may inform the source provider of the case using the re-identification code, the provider may identify the patient, and take whatever action is appropriate, including reporting the identified case to the public health department under the regular mandatory case reporting provisions.

If no re-identification code is available, then it may be possible for a provider organization to infer who the patient of interest is. For example, based on the log of transmissions, or if a disease case is detected at a health department via de-identified laboratory data, then the health department could demand that the provider organization review its own laboratory data to uncover the case.

The matching of patient data is similar. Those mechanisms that allow direct patient identifiers support the matching of patients across health care providers, at least within the limits of data accuracy and completeness. For the other mechanisms, HIPAA does not explicitly support the matching of patients across

health care providers, but its re-identification provisions can be used. De-identified data could in theory be matched if the re-identification codes were coordinated across institutions. This might be possible by having all the health care providers in an area share a common security broker (via a business associate agreement) that generates unique re-identification codes and maintains them.

A limited data set is slightly more flexible. It may include a code that is derived from patient identifiers as long as there is no direct way to reconstitute the patient identifier directly from the code.[20] One such example of a code is a "perfect one-way hash."[21] A one-way hash function is an approved mathematical algorithm that produces a character string (a "hash") for any given input string, but which cannot be reversed; that is, the original input cannot be reproduced from the hash. A "perfect" one-way hash function is one in which the generated hash is unique: two different inputs never map to the same hash. Therefore, a perfect hash of some combination of the patient name, gender, date of birth, social security number, etc. would produce an identifier that is unique to each patient but that would not reveal the patient's identity. If the providers use the same hash function, then when the same demographic data are entered at two different providers, then the hash of those data will be identical, and records from the two providers can be matched. In practice, this method is likely to be less reliable than either a direct match on patient identifiers or the use of a common security broker, however, because demographic data are frequently entered with minor deviations and any deviation will result in a complete mismatch of the hashes. It is possible that even a modest match rate may be adequate for surveillance, which relies on aggregate results.

HIPAA Accounting of Disclosures

The HIPAA generally requires an accounting of disclosures of protected health information, which means that health care providers must keep track of disclosures and report them to patients when requested. Disclosures required by law, disclosures to public health authorities, and disclosures for research do require accounting, whereas disclosures of de-identified information and of limited data sets do not. Expanded public health surveillance may require institutions to keep track of every disclosure (e.g., every real-time data transfer to the health department for each patient).

The HIPAA provides for summary accounting of multiple disclosures (HIPAA Section 164.528(b)(3))[8] that is intended to simplify accounting, although there is some controversy about its interpretation.[22] It states that when multiple disclosures are made to the same entity for the same purpose, then one need only report details of the first disclosure during the accounting period of interest; the frequency, periodicity, or number of disclosures during the period; and the date of the last disclosure during the period.

The Centers for Disease Control guidance on HIPAA[10] states that the multiple disclosures can span multiple patients. The best form of accounting remains unclear. For example, an easy form of accounting would be to record detailed information for the first report of a given purpose since the HIPAA Rule came into effect, the periodicity of **potential** disclosures (for example, reports are potentially sent daily), and the last date of a **potential** disclosure (for example, the last day of the accounting period). Taking the section more literally, however, the provider would need to know the first actual disclosure during an arbitrary accounting period, the actual number of disclosures during the period, and the date of the last actual disclosure. These data would probably have to be derived from a detailed accounting record, so little would be saved in record keeping. A range of interpretations has been noted.[22–26]

At the very least, Section 164.528(b)(3) ensures that when disclosures are reported to patients, a detailed transaction log for that patient need not be printed out (even if it is tracked). Instead a brief summary will suffice.

Approaches to Reporting

Given the above requirements and the HIPAA implications, we describe several approaches to public health reporting:

1. **Mandate disclosure of all identified clinical data by law or by regulation**
   Disclosures required by law are not limited by HIPAA other than its accounting requirements. All the requirements of public health reporting are met in this model because all identifiers may be disclosed. Nevertheless, communities have their own implicit minimum necessary traditions, and it is unlikely that many communities will choose to expand mandated reporting to include all identified clinical information by all providers on all patients. Law and regulation are the primary mechanisms used in the reporting of specific public health conditions, but they are unlikely to be appropriate for very broadly defined surveillance.
2. **Public health authority demand disclosure of identifiable clinical data**
   A public health authority who is legally authorized to receive non-specifically mandated reports may demand the disclosure of identified, or potentially identifiable, clinical information for a specific public health purpose, such as an epidemiological investigation. The HIPAA requires that such disclosures meet the minimum necessary standard and places the responsibility for the determination of minimum data necessary with public health authority.[10] This approach is not appropriate for forms of public health reporting that do not require identifiable patient information.
3. **Providers disclose only de-identified data to the public health authority**
   For certain surveillance purposes, such as for population-level quality measurement, de-identified data may suffice. As described above, using a security broker to generate common re-identification codes, it might be possible to create a model in which de-identified data can also be matched across source facilities and re-identified when necessary. Nevertheless, three-digit zip codes and dates limited to year may limit its use for many types of surveillance. Therefore, the use of de-identified data is unlikely to be the only model for broadly defined surveillance. Furthermore, if data uploads are real-time, then the date of the upload will reveal the date of the visit, rendering the data identifiable according to HIPAA.
4. **Disclose identified clinical data as a research project with Institutional Review Board approval**

In a true research study, one or more Institutional Review Boards should monitor the progress of the study not just for privacy but also for all research ethics issues. Those projects that require approval because they constitute a form of research must do so. It would not be appropriate, however, to designate non-research activities as research for the purpose of circumventing HIPAA.

5. **Providers disclose a limited data set**
   Given a set of data use agreements between a public health authority and each provider in an area, it is possible to support expanded public health reporting with a limited data set, including dates and five-digit zip codes. As described above, using a perfect one-way hash of patient name, gender, and date of birth, it may also be possible to match patients across providers. The match is likely to be inferior to a match based on identified data or a match achieved via a common security broker, but it may be sufficient for surveillance purposes. Re-identification can either be accomplished by having providers maintain a list of the perfect hashes that they reported, or by supplying an additional code. In cases where providers maintain a log of all data transfers (which is not mandated by HIPAA in this case, but might be used for other purposes), then the timestamp of the log record could be used for re-identification. This model appears to meet the requirements for many expanded public health reporting projects unless more detailed addresses are needed.
6. **Distributed surveillance and central aggregation**
   One goal of expanded public health reporting is to enable surveillance based on a wide variety of routine clinical data that would not normally be reported to the health department (e.g., routine signs, symptoms, laboratory results, etc.). Instead of having routine data sent to the health department, one could distribute surveillance activities to providers or regional health information organizations. The providers could implement syndromic case definitions locally and report aggregate statistics.[27] If the goal is monitoring the quality of care in a region, then providers can report aggregate quality statistics. While this solves many of the HIPAA issues, the burden of data transformations, classification, and aggregation would fall on data providers.
   Distributed surveillance may qualify as de-identified data if aggregate counts are sufficiently large that individuals cannot be identified. For example, if the public health authority can ask a provider to query for all newly diagnosed (within one day) HIV patients of a certain age in a certain zip code, and the provider returns a count of one, then the diagnosis date, zip code, and age of an HIV patient has been disclosed. This may be addressed by setting a minimum reportable count or by adding random noise to the counts.

Discussion

Expanded public health surveillance will probably follow several approaches to accommodate the variety of needs. Modest expansions of traditional public health reporting may be most easily implemented by creating law or regulation that mandates identified reporting (approach 1). For example, regulations direct the New York City Department of Health and Mental Hygiene to collect hemoglobin A1c results to monitor the quality of diabetes care in New York City.[28]

In cases where expanded public health goals (i.e., non-mandated reporting, rather than traditional public health reporting for such things as outbreaks) can be accomplished without patient identities, safe harbor de-identification (approach 3) and aggregation at the source facilities (approach 6) may be useful. It may be possible to use approach 6 by applying surveillance functions at the level of the virtual medical record or by pushing surveillance to the provider organizations via software distributed by a regional health information organization. Where public health goals require more detailed information, limited data sets may provide a balance between privacy and public good (approach 5).

The most ambitious project for expanded public health reporting in the nation is BioSense.[29] The Centers for Disease Control and Prevention (CDC) is receiving clinical data from the Veterans Administration and Department of Defense hospitals and clinics, commercial laboratories, and health care facilities around the nation for the purpose of public health surveillance of bioterrorism, disease outbreaks, and natural disasters. BioSense has been seeking all data related to "non-identifying patient demographics, diagnoses, chief complaints, microbiology orders/results, radiology orders/results, medication orders, laboratory orders/results, and pharmacy data" including dates and 5-digit zip codes.[30] The CDC has been seeking all related data within those categories, relying on the CDC's designation as a public health authority and broadly worded legislation that provides for the "the establishment of an integrated system or systems of public health alert communications and surveillance networks between and among—(A) Federal, State, and local public health officials; (B) public and private health-related laboratories, hospitals, and other health care facilities; and (C) any other entities determined appropriate by the Secretary"[31] to justify the collection of clinical data. This appears to be consistent with approach 5, and CDC has been entering into a data sharing agreement with each data source. The CDC explicitly justifies its selected data elements as being the minimum necessary needed for BioSense's mission.[30]

In summary, expanded public health surveillance faces a number of challenges related to patient privacy and confidentiality. The HIPAA provides mechanisms to address some of the challenges, although the exact method will vary with the context. Some issues, such as how disclosures must be accounted for, remain unclear. Different combinations and implementations of the approaches defined here will likely be developed in the future.

References ■

1. Delaware Health and Social Services. Historical Development of Morbidity Reporting and Surveillance in the United States. Available at http://www.dhss.delaware.gov/dhss/dph/epi/historydisrpt.html; accessed May 12, 2008.
2. Centers for Disease Controal. Nationally Notifiable Infectious Diseases. Available at http://www.cdc.gov/epo/dphsi/phs/infdis2006.htm; accessed May 12, 2008.
3. National Office of Vital Statistics. MMWR Morbidity and mortality weekly report. 1952;1(1).
4. Nguyen TQ, Thorpen L, Makki HA, Mostashari F. Benefits and Barriers to Electronic Laboratory Results Reporting for Notifiable Diseases: The New York City Department of Health and Mental Hygiene Experience. Am J Public Health 2007;97:S142–S145.

5. Shapiro JS, Kannry J, Lipton M, et al. Approaches to patient health information exchange and their impact on emergency medicine. Ann Emerg Med Oct 2006;48(4):426–32.
6. DeBor G, Diamond C, Grodecki D, Halamka J, Overhage JM, Shirky C. A tale of three cities—where RHIOS meet the NHIN. J Healthc Inf Manag Summer 2006;20(3):63–70.
7. Mandl KD, Overhage JM, Wagner MM, et al. Implementing syndromic surveillance: a practical guide informed by the early experience. J Am Med Inform Assoc 2004;11:141–50.
8. Office for Civil Rights, Department of Health and Human Services. Title 45 of the Code of Federal Regulations Parts 160 and 164. Available at http://www.dhhs.gov/ocr/combinedregtext.pdf; accessed May 12, 2008.
9. Gostin LO. Health information: reconciling personal privacy with the public good of human health. Health Care Anal 2001;9(3):321–35.
10. Centers for Disease Control and Prevention. HIPAA privacy rule and public health. Guidance from CDC and the U.S. Department of Health and Human Services. MMWR. 2003; 52(suppl):1–20. Available at http://www.cdc.gov/mmwr/pdf/other/m2e411.pdf; accessed May 12, 2008.
11. Sweeney L. Weaving technology and policy together to maintain confidentiality. Journal of Law, Medicine and Ethics 1997; 25:98–110.
12. Sweeney L. k-anonymity: a model for protecting privacy. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems 2002;10(5):557–70.
13. Malin BA, Sweeney L. A secure protocol to distribute unlinkable health data. AMIA Annu Symp Proc 2005;:485–9.
14. Olson KL, Grannis SJ, Mandl KD. Privacy protection versus cluster detection in spatial epidemiology. Am J Public Health. Nov 2006;96(11):2002–8.
15. Cassa CA, Grannis SJ, Overhage JM, Mandl KD. A context-sensitive approach to anonymizing spatial surveillance data: impact on outbreak detection. J Am Med Inform Assoc 2006;13: 160–5.
16. Sweeney L. Guaranteeing anonymity when sharing medical data, the Datafly System. Proc AMIA Annu Fall Symp 1997;: 51–5.
17. Broome CV, Horton HH, Tress D, Lucido SJ, Koo D. Statutory basis for public health reporting beyond specific diseases. J Urban Health 2003 Jun;80(2 Suppl 1):i14–22.
18. Lopez W. New York City and state legal authorities related to syndromic surveillance. J Urban Health 2003 Jun;80(2 Suppl 1):i23–4.
19. The Impact of the HIPAA Privacy Rule on Syndromic Surveillance. Association of State and Territorial Health Officials, 2004. Available at http://www.hhs.gov/healthit/ahic/materials/meeting04/bio/impHIPAAprivrulsyndsurvastho.pdf; accessed May 12, 2008.
20. The Federal Register: August 14, 2002 (Volume 67, Number 157). Available at http://www.dhhs.gov/ocr/hipaa/privruletxt.txt; accessed May 12, 2008.
21. Cormen TH, Leiserson CE, Rivest RL, Stein C. Introduction to Algorithms, Second Edition. MIT Press and McGraw-Hill, 2001: 245–9.
22. Testimony of James J. Gibson MD, MPH, to the Subcommittee on Privacy and Confidentiality of the National Committee on Vital and Health Statistics. Available at http://www.ncvhs.hhs.gov/031119p2.htm; accessed May 12, 2008.
23. Department of Health and Human Services National Committee on Vital and Health Statistics Subcommittee on Privacy and Confidentiality. Meeting Minutes of November 19–20, 2003. Available at http://www.ncvhs.hhs.gov/031119mn.htm; accessed May 12, 2008.
24. Advancing Health in America. Improving the HIPAA Accounting for Disclosures Requirement. Avaliable at http://www.hospitalconnect.com/aha/key_issues/hipaa/content/AHAFAQsonaccountingofdisclosures.doc; accessed Dec 31, 2005.
25. Minnesota Department of Health. Frequently Asked Questions about Sexually Transmitted Disease (STD) Reporting. Available at http://www.health.state.mn.us/divs/idepc/dtopics/stds/stdreportingfaq.pdf; accessed May 12, 2008.
26. Georgia Department of Human Resources (DHR) Division of Public Health HIPAA Fact Sheet: Emergency Medical Services. Available at http://health.state.ga.us/pdfs/publications/factsheets/emshipaafactsheet.04.pdf; accessed May 12, 2008.
27. Platt R, Bocchino C, Caldwell B, et al. Syndromic surveillance using minimum transfer of identifiable data: the example of the National Bioterrorism Syndromic Surveillance Demonstration Program. J Urban Health 2003 Jun;80(2 Suppl 1):i25–31.
28. Steinbrook R. Facing the diabetes epidemic—mandatory reporting of glycosylated hemoglobin values in New York City. New England Journal of Medicine 2006;354:545–8.
29. Bradley CA, Rolka H, Walker D, Loonsk J. BioSense: implementation of a National Early Event Detection and Situational Awareness System. MMWR Morb Mortal Wkly Rep 2005 Aug 26;54 Suppl:11–9.
30. Centers for Disease Control and Prevention. BioSense FAQs. Available at http://www.cdc.gov/biosense/faqs.htm; accessed May 12, 2008.
31. HR 3448. Public Health Security and Bioterrorism Preparedness and Response Act of 2002, Sec. 108. Available at http://www.fda.gov/oc/bioterrorism/PL107-188.html; accessed May 12, 2008.