Syndromic Surveillance and Patients as Victims and Vectors

Leslie P. Francis, Margaret P. Jacobson, Jay Jacobson, & Charles B. Smith

Protection of populations from infectious disease requires effective surveillance to identify diseases and disease trends. The better the surveillance, the more quickly outbreaks can be identified and contained. This is especially important for a rapidly spreading condition with high levels of mortality and morbidity, as human-to-human pandemic influenza is thought likely to be. Yet there are many barriers to effective surveillance, including inadequate public health systems, limited resources, reluctant population groups, and ethical objections. In this contribution, we discuss how an ethical perspective we have developed—what we call “the patient as victim and vector,” or “PVV” for short (Battin et al. 2009)—can help in analyzing ethical concerns about a new and important form of surveillance: so-called “syndromic surveillance”, that employs a variety of innovative information technologies to monitor for clusters of symptoms or complaints.

Several ethical concerns have been thought to apply to syndromic surveillance. These include the possibility that access to individuals and collection of information from them may occur without their consent; the potential for loss of privacy and confidentiality; and, the risk that individuals or groups may be stigmatized, physically harmed, or otherwise victimized by the information collected. There are political concerns as well: the establishment of novel data-gathering means without public knowledge, decision-making or oversight. On our PVV perspective, we conclude that robust surveillance regimes of the type envisioned by syndromic surveillance can only be ethically justified, despite their anticipated benefits, if they are accompanied by attention to the victim-needs of those about whom data are obtained. These victim-needs include transparency and oversight, protection from harm, and access to preventives or treatment to the extent possible, but do not extend to informed consent or protection of privacy in every instance. In considering the ethical issues raised by syndromic surveillance, moreover, it is especially important to distinguish privacy as access to individuals in the initial information-gathering encounter, and confidentiality as protection of the transfer of identifying or identifiable information about them.

Traditional Surveillance and Syndromic Surveillance

Surveillance has been called the “backbone” of public health efforts in disease prevention and control (Gostin and Berkman 2007, 155). Individual case surveillance identifies people with particular diseases (such as tuberculosis or syphilis) and provides the option to intervene to treat and to stop spread. In its traditional form, such case surveillance involves specification of a list of “reportable” diseases to an entity such as a department of health, followed by treatment and/or contact tracing as deemed necessary. It also involves reporting or monitoring of laboratory testing results for identified organisms, toxins, or other suspected agents of disease. In complement, statistical
surveillance identifies disease trends in populations: incidence, prevalence, distribution, and the like (Stoto 2008).

These traditional surveillance methods begin with a determination of the diagnoses, or agents of disease, that are thought to be of public health interest. For example, the World Health Regulations in effect until 2007 required reporting of cholera, yellow fever, and plague—but only these three diseases (Chretien et al. 2008). In the United States, under the National Notifiable Diseases Surveillance System (NNDSS), disease surveillance at the federal level has been voluntary, and based on case reports under reporting systems mandated at the state level and alerts from clinicians and laboratories about disease clusters (Centers for Disease Control). At the state level, public health statutes typically require reporting of specified infectious diseases (NYCLS PUB HEALTH § 2130 2008), cancer diagnoses (e.g., CALIFORNIA HEALTH & SAFETY CODE [DEERING’S] § 103885 2008), workplace toxins (MINN. STAT. § 175.33 2008), and more recently agents associated with bioterrorism (ARIZ. REV. STAT. § 36-782 2008). Other recent proposals have extended surveillance beyond contagious disease and environmental toxins, the traditional domains of public health, to identify incidence and prevalence of diseases such as diabetes—an expansion that has come under criticism (Mariner 2007).

However, with emerging contagious diseases such as HIV or SARS, new strains of influenza, or as-yet-to-be-imagined agents of bioterrorism, illness may reach pandemic proportions if effective surveillance must wait upon identification of a diagnosis or disease-causing agent that is the object of interest. Instead, observation and subsequent investigation of behavioral or symptom patterns of potential significance is an important way of ascertaining a developing public health threat. The basic idea of such “syndromic surveillance” is to collect real-time data about disease indicators in order to detect possible outbreaks of diseases even before the diseases themselves have been identified (Buehler et al. 2004; Mandl et al. 2004). Syndromic surveillance thus relies on a wide variety of data available in electronic or other forms beyond those used in traditional surveillance (Chretien et al. 2008; Heffernan et al. 2004). This includes information such as data about chief complaints, symptoms, medication sales; grocery store purchases such as pediatric electrolyte formulas or even orange juice; absenteeism from work or school; or internet queries for topics such as “influenza” or “fever.” For example, an important data source in syndromic surveillance is emergency room visits. One of the measures of disaster preparedness employed in the American College of Emergency Physicians’ report card on the status of emergency medicine in the United States is the presence of real-time surveillance systems for common emergency department presentations (American College of Emergency Physicians 2009). As an illustration, North Dakota receives daily electronic feeds of chief complaint data from eight large emergency rooms in the state (North Dakota Health Department). Such feeds can alert public health officials about unusual clusters or increased rates of symptoms such as diarrhea, respiratory illness, or joint pain—and trigger further investigation about what might be causing the observed phenomena. In Europe, syndromic surveillance has been developed quite extensively (Smith et al. 2006; Josseran et al. 2006).
Syndromic surveillance, as thus understood, is based on novel data sources and
data-mining techniques: emergency department data in electronic form, electronic
medical records, electronic prescription data, pharmacy purchases, reported absenteeism,
and traffic on the web in particular (Sengupta, Calman, and Hripcsak 2008; Mandl et al.
2004). Such surveillance presents new possibilities and new challenges. One difficulty in
the construction of syndromic surveillance techniques is validation: for example, is an
increase in certain pharmacy purchases indicative of a rise in respiratory disease? (One
study concludes that it is (van den Wijngaard 2008).) Other studies have concluded that
reports of respiratory symptoms in pediatric emergency rooms are indicative of a rise in
respiratory syncytial virus (Bourgeois et al. 2006). On the other hand, purchases of
antivirals may be generated by individual decisions to stockpile after publicity about
influenza, rather than with any increased rates of influenza itself (Centers for Disease
Control 2006). Concerns have also been raised about the accuracy of syndromic
surveillance at single institutions; however, the problem may be limited data rather than
methodological difficulties with syndromic surveillance per se (Weber and Pitrak 2003).
Even when measures are validated, sensitivity and specificity pose additional problems. It
is desirable to have highly sensitive measures to avoid missing detection of potentially
serious outbreaks, but this raises concerns about false positives and attendant costs and
risks (Buehler et al. 2004).

Several features of syndromic surveillance are particularly noteworthy for ethical
purposes. With traditional reporting systems, conditions of interest are identified in
advance. This identification is typically codified by legislative action or administrative
rule-making. There has thus been a degree of public oversight of the decision to make a
disease reportable. However, as we detail below, even recent and proposed reforms of
public health law have not anticipated the full range of possibilities syndromic
surveillance may present. Thus as it has developed to date, syndromic surveillance has
not been subject to the level of public scrutiny that has attended traditional public health
surveillance. Legally-established reporting regimes typically also implement
mechanisms for protecting the confidentiality of any reported data, but comparable
regimes have not been fully developed for protecting the data obtained for purposes of
syndromic surveillance.

Moreover, because in traditional surveillance the need for reporting is identified
in advance, informed consent discussions of health care providers with their patients can
include any relevant reporting requirements. A physician recommending testing to a
patient for HIV or syphilis can explain the significance of a positive test result before the
patient agrees to the test. With new methods of syndromic surveillance, by contrast,
issues of informed consent and data use are far less well analyzed and understood. As it
involves the identification of patterns of interest, patients and providers may not know in
advance that a particular symptomatic report entered into an electronic medical record
will be of any significance whatsoever: whether this fever triggers interest may only be
known after a pattern of fevers is observed in an interoperable set of electronic records.
Moreover, no informed consent process at all is involved in such activities as purchase of
an over-the-counter anti-diarrheal or a search of the web for information about managing
fever.
Some syndromic surveillance collects electronically-stored data that includes identifying information about individual patients, allowing for possible investigation if patterns of concern are identified (Nordin et al. 2008). Such data collection practices pose risks to patient confidentiality if data security is imperfectly protected (Myers et al. 2008). To be sure, some syndromic surveillance in the United States involves “de-identified” electronic health data, health records from which a defined list of identifying information has been removed as set out in the federal privacy rule for medical information transmitted in electronic form (HIPAA 2008). However, increasingly concerns have been raised about whether de-identified data can be readily re-identified, especially when data sets are combined (Porter 2008), as data sets are likely to be under robust syndromic surveillance regimes. Consider, for example, combining electronic medical records, pharmacy purchase data, and grocery store purchases of over-the-counter remedies using a frequent-shopper discount card that contains purchaser identifying information. Moreover, entities issuing de-identified data sets may keep coded identifiers to permit re-identification in case of public health need (Sengupta, Calman and Hripcsak 2008). Thus there may be risks to patient confidentiality even when de-identified data sets are employed for syndromic surveillance. These very real risks to confidentiality highlight the importance of careful consideration of regimes for data protection if syndromic surveillance is to be employed.

Even when re-identification of individual patients is unlikely, syndromic surveillance may pose risks of stigmatization of both groups and individuals whose group membership is known (National Committee on Vital and Health Statistics 2008, 4). This is of particular concern given the imperfect validation of syndromic surveillance techniques, as well as the risks of false positives when the emphasis is placed on detection methods with high sensitivity (Stoto, Schonlau and Mariano 2004). Syndromic surveillance may identify suspected higher rates of illness or disease risk in particular populations. One quite recent example of group stigmatization involved an HIV exposure alarm among students at a particular school (whose school population happened to be 99% African-American) (Gay 2008). Stigmatization has also been alleged concerning minority patients with diabetes in New York City (Goldman et al. 2008). The untoward result may be prejudicial to everyone who meets the given description, without regard to the accuracy of the initial suspicions and without concern for them as people, too.

But there is surely more to come than the syndromic surveillance methods we have seen to date. The data collection in syndromic surveillance, as it has developed so far, is just the beginning. Surely, as more robust systems of electronic health records are put into play, more extensive data mining for public health purposes will come into play. But there is more. Consider the thought experiment—or perhaps realistic proposal—that we developed elsewhere: universal rapid testing for infectious disease in airports, on public transit, at schools, workplaces, movies and sporting events (Battin et al. 2009, Ch. 15). Or suppose that it were possible to detect overall temperature levels in a population by means of remote thermal imaging. Suppose this could be done in such a way that no one was aware that data were being collected and no information about particular
individuals was included in the data collection. All that was ascertained was the occurrence of shifts in the amount of heat emitted by bodies of a given size in a particular area. Such sensing is a technologically possible method for determining whether there has been an increase in bodily temperatures in a population—and a possible method for determining whether a corresponding rise in infection rates has been occurring in a population. Although remote thermal sensing of people while they are in their homes would likely be an unreasonable search and seizure under United States law, this use of thermal imaging could be a very effective way of ascertaining increased rates of infectious disease in a population, perhaps even more effective than monitoring data about purchases of aspirin or acetaminophen in local pharmacies.iv

Syndromic Surveillance and the Patient as Victim and Vector

A central goal of surveillance is to identify threats to the public health so that effective intervention can take place. With transmissible disease, surveillance focuses on the individual as a source of illness to be identified and contained, or as a source of information about transmission. In the language of the analysis we have developed elsewhere, that of the patient as “victim and vector,” an aspect of surveillance is to regard everyone as potential vectors from whom society is to be protected. Syndromic surveillance is no exception to this generalization.

As we have argued, however, the field of bioethics has been impoverished by the failure to attend to persons as both victims and vectors (Battin et al. 2009). As human animals, we are way stations for microbial transmission, biologically interrelated in networks of organism interchange. Seen from the perspective of our ordinary lives, we are more-or-less susceptible to infection: some are immune-compromised, some already ill, some in conditions of poverty where disease transmission is especially high and susceptibility is great, and some protected by living in conditions of apparent relative safety. However, there is a sense in which no one is immune: we are all potentially victims and vectors to each other, unknown and unknowingly. As victims, we are concerned that vectors may transmit illness to us; but as vectors, we are victims too. We exist behind what might be thought of as an infectious-disease veil of ignorance; our ethical judgments must come to terms with this feature of our human condition. This is not a matter of mere self-interest, requiring us to calculate from our own particular circumstances how likely infection is to occur. It is a deeper metaphysical point: both the victim and vector perspectives belong to everyone, all of the time.

To the extent that it is effective in detecting potentially dangerous disease—an improvement on other surveillance techniques—syndromic surveillance would be defensible from the perspective in which we do not know whether we are victims or vectors. It should be emphasized that this justification is contingent on the efficacy of syndromic surveillance: if syndromic surveillance raises insurmountable technical difficulties, cannot be validated, is less sensitive or specific than other surveillance methods, or even poses greater risks than these other methods for limited or no improvement, it would not be justified out of concern to protect ourselves from potential vectors. But even if syndromic surveillance is justified as a means for preventing disease
spread, this is not the end of the ethical story; any such justification would also warrant attention to ourselves as victims, in a number of respects.

First of all, as victims we would want to be sure that surveillance is not more extensive than apparently needed to detect outbreaks of potentially serious disease. Widespread “fishing” expeditions of uncertain validity would be unacceptable to us as victims. Otherwise, the risks to ourselves as victims who are affected by surveillance might be greater than the gains to ourselves in being protected from potential vectors. But this requirement of narrow tailoring is just a beginning.

Additionally, as vectors who are also potential victims we would want assurance that we are protected to the extent possible in the course of whatever surveillance takes place. Such protection starts by subjecting surveillance methods to public oversight. At a minimum, there must be transparency about what is happening with respect to surveillance: public knowledge of what surveillance is taking place and how it is being conducted. Without such transparency, immense amounts of data may be collected about people, combined and recombined, without any public knowledge of what is happening whatsoever. There should as well be some kind of public decision making process—legislation or administrative rule-making, for example—to scrutinize and accept the surveillance process. Finally, there should be public oversight of surveillance: a mechanism for assessing whether methods being employed are appropriately limited to need, and that people are informed if there are breaches of guarantees such as confidentiality.

Arguably, such public knowledge and oversight is the best available substitute for an informed consent process on the individual patient level. If there is full public information about what surveillance is being done, as well as oversight through the political process, then the political process might be viewed as analogous to community consent of the form utilized in research when subjects cannot be identified in advance (McClure et al. 2003). However, it is important to note that so-called “community consent” models as they are currently implemented may fail to communicate adequately with community members about planned research. As victims, we would want to insist that syndromic surveillance be fully vetted at the political level, and that there be ongoing public oversight to ensure that safeguards are employed as promised.

One of the most serious objections to any surveillance is patient privacy and confidentiality. As we have already indicated, the novel uses of data in syndromic surveillance may place serious pressures on confidentiality. To take just one example, if a novel influenza strain appears as it apparently did in the spring of 2009, intense efforts may be devoted to identifying and detaining air travelers with potential exposures (Centers for Disease Control 2008). Although these two concepts are often used interchangeably, privacy refers to the initial intrusion—the contact from which data are obtained—and confidentiality refers to individual control over the information thus obtained. From the victim/vector perspective, it is not clear that privacy is the more important value. Protection from each other as vectors may be significantly inadequate without the initial access that allows data to be gathered. At the same time, if
confidentiality is not protected and people are identified, then risks of harm may be significant. These risks stem from the information becoming known, not from its being gathered in the first place; the only likely harm, for example, from a grocery store keeping an electronic record of an aspirin purchase, even a purchase linked to a particular individual, might be identification of that individual as being ill. The reason for protecting privacy is not the harm involved in the moment of data gathering; it is instead the concern that, once gathered, the data will inevitably come to light. To put the point succinctly, confidentiality is the reason for protecting privacy, not the reverse (Francis 2008).

Because of the more extensive threats to confidentiality involved in syndromic surveillance, reconsideration of what data confidentiality and security require in this context is especially urgent. As victims, we would like to be assured that we will not be publicly identified as disease threats—and that if we are identified at all, it will be for our own protection. This requires assurance that when a disease threat is determined and individuals must be contacted, as when codes are broken with de-identified data sets to all for individual contact, the contact will include offers of treatment—or if treatment is not yet a possibility, with assurances of protection from harm to the extent possible. It also requires assurance that we will be told if confidentiality is ever breached in this or other ways, so that we may know about the need for protection and be able to take steps to avoid harm from the confidentiality breach.

Finally, as victims we will also be concerned about risks of stigmatization. To some extent, transparency and political oversight can help to modulate these risks. But the risks remain, at least in a world in which fear and prejudice have not been forgotten. One critic of New York City’s surveillance for diabetes argued that these risks of harm demand that surveillance be coupled with the availability of resources for prevention and treatment.

These initiatives do not balance heightened surveillance and intervention with the provision of meaningful safeguards or resources for prevention and treatment. The programs intrude on the doctor-patient relationship and may alienate the very patients and health professionals they aim to serve. (Goldman et al. 2008)

One way to blunt or mitigate the risks of stigmatization is to make prevention and treatment available as a complement to surveillance activities—to everyone, to the extent possible. If prevention and treatment are available, people will have less reason to fear and to regard others as ones-to-be-feared. Moreover, prevention and treatment are what people have to gain from the risks of having data about them be used in efforts to identify disease early on.

Nonetheless, the most difficult cases are those in which prevention and treatment are not available, because supplies are scarce, treatment is very expensive, or treatment has yet to be developed. With pandemic H5N1 influenza, this is exactly the fear: that it will be highly lethal and that anti-virals will prove ineffective. As victim-selves, the best we can do in such circumstances is to cooperate in efforts to stop disease at the earliest
point. Thus we would support syndromic surveillance if it seems likely to be effective. But we would want the oversight to be very careful indeed—with ongoing attention paid to what surveillance techniques are being employed and whether they continue to be needed or effective. And we would want society to continue to be engaged in the project of considering how to respect people who are victims of disease, even if their conditions cannot be ameliorated.

**Syndromic Surveillance and the New International Health Regulations**

Although the need for reform of public health laws has been widely recognized, especially in the wake of fears of pandemic influenza and the realities of SARS and 9-11, reforms that have been enacted may not have caught up fully with the possibilities of syndromic surveillance. Legal regimes governing surveillance function at many different levels, from the World Health Organization to the very local. Here we give a snapshot of recent reforms in the WHO International Health Regulations that are important but that may not grapple with the full ethical implications of syndromic surveillance. Although these reforms contemplate more extensive and effective surveillance, they are non-specific about whether what is contemplated is a wider range of traditional disease surveillance or shifts to syndromic surveillance.

In June of 2007, the new International Health Regulations went into effect. These Regulations require states parties to meet specified functional requirements for surveillance. “Surveillance” in the Regulations is defined as “the systematic ongoing collection, collation, and analysis of data for public health purposes.” (International Health Regulations, art. 1) The Regulations thus represent an enormous advance over the prior regulations, which only required reporting of three identified diseases: cholera, yellow fever, and plague. At the local level, functional requirements include the capacity to detect events involving disease or death above expected levels in all areas of the territory (International Health Regulations, Annex I). They also include the ability to report available information to the relevant response level—information including clinical descriptions, laboratory results, sources and types of risk, numbers of human cases and deaths, conditions affecting spread, and health measures taken. Local authorities are also expected to be able to implement preliminary control measures immediately. At the intermediate level, requirements include confirmation of the status of events and the ability to support or augment control measures. They include, in addition, assessment of the urgency of the situation and the ability to transmit information about any urgent situations to national authorities. National authorities, in turn, must be able to assess events reported as urgent and to report as necessary to the WHO. They must also be able to provide adequate public health responses on a 24-hour basis.

These are clearly extensive requirements and may be difficult to meet in economically challenged areas of the world. In recognition, the Regulations also commit more affluent states parties to help the less affluent to comply with the requirements. They also permit a two-year grace period for implementation generally, and longer periods for compliance with requirements such as adequate response capability. As of February 2008, all 194 nations were states parties to the IHR.
Notably, the United States has become a state party under a reservation: the insistence on implementing the regulations consistently with federalism. Three limiting “understandings” were also submitted by the United States: that the notification requirements apply whether the emergency is natural or human-caused in origin; that the requirement to report if “practicable” known emergencies outside the country’s territory does not apply in cases that would jeopardize the effective operation of U.S. armed forces; and that the IHR do not create enforceable private rights of action (http://www.who.int/csr/ihr/states_parties/en/index.html).

Although the new Regulations are widely regarded as a major step forward, concerns remain. These include the lack of technical capacity to implement the regulations, issues of resource allocation, concerns about privacy, and questions about overall governance (PLoS Medicine Editors 2007; Baker and Fidler 2006). The editors of PLoS Medicine, for example, point out that most of the investment in preparing for pandemic influenza has involved stockpiling resource in developed countries (PLoS Medicine Editors 2007). Other discussions praise the wider reach of the regulations about what are regarded as events of public health significance, but also express concern about whether the investment will be there to build the technical capacity for the required surveillance (Sturtevant, Anema and Brownstein 2007).

Despite the advances they represent, it is controversial whether the Regulations in their final form are meant to include the capacity for syndromic surveillance. Baker and Fidler (2006) contend that although syndromic surveillance was discussed, the decision was not to include it in the Regulations because of concerns about validity. However, in fashioning the requirements for surveillance and reporting, the Regulations define a public health emergency of international concern as “an extraordinary event which is determined . . . to constitute a public health risk to other states through the international spread of disease and to potentially require a coordinated international response” (International Health Regulations, art. 1). This definition elides whether the reference is only to identified diagnoses or agents or includes syndromic identification as well. Although the definition of “surveillance” quoted above is surely broad enough to include syndromic surveillance, nothing more specific is stated about the possibilities. In discussing the resource issues raised by the Regulations, Chretien et al. (2008) give illustrations of successful establishment of syndromic surveillance capacity in Indonesia and Peru. It seems increasingly likely, moreover, that as syndromic surveillance techniques become better developed, pressures will increase for their use in detecting emerging disease before spread becomes likely—especially, we might hypothesize, spread to more affluent areas of the world.

Thus if the Regulations encompass syndromic surveillance, they are insufficiently attentive to the ethical issues we have raised. The Regulations state that all measures should be implemented in a transparent and non-discriminatory manner (International Health Regulations, art. 42), but do not set out any specific requirements for what this might involve. With respect to privacy, Article 45 states both that data should be processed anonymously and that personal information may be used when needed, so long as they are processed fairly and not kept longer than necessary (International Health
Regulations, art. 45). These provisions are quite vague, however, and do not attend specifically to the privacy and confidentiality issues that may be raised by increasing use of non-traditional forms of surveillance. Although the Regulations commit more affluent countries to helping others in developing surveillance capacities (International Health Regulations, art. 44), they do not include commitments to more extensive development of the health infrastructure needed to ensure that treatment is available to the extent possible for those who are identified as disease threats.

**Conclusion**

So-called “syndromic surveillance” poses novel and unexplored possibilities for protection from disease, protection that as victims we would find especially important when diseases are severe and treatments are unknown or inadequately distributed. However, because of the risks to confidentiality and concerns about stigmatization, data use in syndromic surveillance may pose more extensive risks to perceived vectors than more traditional forms of surveillance. As attempts to monitor for emerging pandemic infections continue to develop, the ethical problems raised by syndromic surveillance will need much further attention.
References

American College of Emergency Physicians. 2009. National report card on the state of emergency medicine. http://www.emreportcard.org/uploadedFiles/ACEP-ReportCard-10-22-08.pdf.pdf.

ARIZ. REV. STAT. § 36-782 (2008)

Baker, M. G. and D. P. Fidler. 2006. Global public health surveillance under New International Health Regulations. Emerg Infect Dis. 12(7): 1058-1065.

Battin, M. P., L. P. Francis, J. A. Jacobson, and C. B. Smith. 2009. The patient as victim and vector: Ethics and infectious disease. New York: Oxford University Press.

Bernhard, B. and S. Giegerich. 2008. State finds no HIV outbreak at Normandy High; County Health Department continues its own investigation. St. Louis Post Dispatch 4 December, C1.

Bourgeois, F.T. et al. 2006. Validation of syndromic surveillance for respiratory infections. Ann. Emerg Med. 47(3):265.e1.

Brown, S. Jr. 2008. Normandy High problem quickly became a racial issue. St. Louis Post Dispatch 26 October, D1.

Buehler, J.W. et al. 2004. Framework for evaluating public health surveillance systems for early detection of outbreaks. MMWR 53(RR05): 1-11. http://www.cdc.gov/mmwr/preview/mmwrhtml/rr5305a1.htm (accessed April 22, 2009).

CALIFORNIA HEALTH & SAFETY CODE [DEERING’S] § 103885 (2008)

Centers for Disease Control, National Notifiable Diseases Surveillance System, http://www.cdc.gov/ncphi/disss/nndss/nndsshis.htm.

Centers for Disease Control. 2008. Federal air travel restrictions for public health purposes—United States June 2007-May 2008. MMWR 57: 1009-1012.

Centers for Disease Control. 2006. Increased antiviral medication sales before the 2005-06 influenza season--New York City. MMWR 55(10): 277-9.

Chretien, J.-P. et al. 2008. Syndromic surveillance: Adapting innovations to developing settings. PLoS Medicine 5(3): e72 doi:10.1371/journal.pmed.0050072 (accessed April 22, 2009).

Francis, L. P. 2008. Privacy and confidentiality: The importance of context. Monist 91(1): 52-67.
Gay, M. 2008. H.I.V. scare unnerves a St. Louis high school. *New York Times*, 9 November 9, A30.

Ginsburg, J. 2008. Detecting influenza epidemics using search engine query data. *Nature* doi:10.1038/nature07634 (accessed April 22, 2009).

Goldman, J. et al. 2008. New York city's initiatives on diabetes and HIV/AIDS: Implications for patient care, public health, and medical professionalism. *Am. J. Public Health* 98(5): 807-13.

Google.org, Flu trends. http://www.google.org/about/flutrends/how.html.

Gostin, L. O. and B. E. Berkman. 2007. Pandemic influenza: Ethics, law, and the public’s health. *Administrative Law Review* 59: 121-175.

Heffernan, R. et al. 2004. Syndromic surveillance in public health practice, New York City. *Emerg Infect Dis.* 10(5): 858-64.

HIPPA. 45 C.F.R.§164.514(b)(2) (2008)

International Health Regulations, http://whqlibdoc.who.int/publications/2008/9789241580410_eng.pdf (accessed April 22, 2009).

Josseran, L. et al. 2006. Syndromic surveillance based on emergency department activity and crude mortality: Two examples. *Eurosurveillance* 11(12): 1 December.

*Kyllo v. United States*, 533 U.S. 27 (2006)

Mandl, K.D. et al. 2004. Implementing syndromic surveillance: A practical guide informed by the early experience. *J. Am. Med. Inform. Assoc.* (Mar-Apr) 11(2): 141-50.

Mariner, W. K. 2007. Mission creep: Public health surveillance and medical privacy. *Boston University Law Review* 87: 347-395.

McClure, K.B. et al. 2003. Attitudes of emergency department patients and visitors regarding emergency exception from informed consent in resuscitation research, community consultation, and public notification. *Acad Emerg Med.* 10(4): 352-9.

MINN. STAT. § 175.33 (2008)

Myers, J. et al. 2008. Ethics in public health research: Privacy and public health at risk: Public health confidentiality in the digital age. *American Journal of Public Health* 98(5): 793-801.

National Committee on Vital and Health Statistics. 2008. Enhancing protection for uses of health data: A stewardship framework. http://www.ncvhs.hhs.gov/080424rpt.pdf (accessed December 13, 2008).
Nordin, J. D. et al. 2008. Bioterrorism surveillance and privacy: Intersection of HIPAA, the common rule, and public health law. *American Journal of Public Health* 98(5): 802-807.

North Dakota Health Department. http://www.ndhealth.gov/Disease/Surveillance/syndromicsurveillance.htm.

PLoS Medicine Editors. 2007. How is WHO responding to global public health threats? *PLoS Med* 4(5): e197 doi:10.1371/journal.pmed.0040197.

Porter, C. C.. 2008. De-identified data and third party data mining: The risk of re-identification of personal information. *Shidler J.L. Com. & Tech.* 5 (Sep. 23). http://www.lctjournal.washington.edu/Vol5/a03Porter.html (accessed December 12, 2008).

Sengupta, S., N. S. Calman, and G. Hripcsak. 2008. A model for expanded public health reporting in the context of HIPAA. *J. Am. Med. Inform. Assoc.* 15: 569-574

Smith, G.E. et al. 2006. A national syndromic surveillance system for England and Wales using calls to a telephone helpline. *Eurosurveillance* 11(12): 1 December.

Stoto, M. A. 2008. Public health surveillance in the twenty—first century: Achieving population health goals while protecting individuals’ privacy and confidentiality. *Georgetown Law Journal* 96: 703-719.

Stoto, M. A., M. Schonlau and L. T. Mariano. 2004. Syndromic surveillance: Is it worth the effort? *Chance* 17(1): 19-24.

Sturtevant, J. L., A. Anema, and J. S. Brownstein. 2007. The new International Health Regulations: Considerations for global public health surveillance. *Disaster Medicine and Public Health Preparedness* 1(2): 117-121.

van den Wijngaard, C. et al. 2008. Validation of syndromic surveillance for respiratory pathogen activity. *Emerg Infect Dis.* 14(6): 917-25.

---

i Google health claims to be able to predict flu trends more quickly than CDC (Ginsberg 2008; Google 2008).

ii HIPAA defines “de-identified data” as data from which 18 identifiers (such as date of birth, social security number, medical record number, telephone number, and so on) have been removed, 45 C.F.R.§164.514(b)(2) (2008). Under HIPAA, data may also be de-identified if statistical analysis determines that the probability of re-identification is very small.

iii For a description of the racial stereotyping that occurred to students at the school, see Brown (2008). Initial indications are that the scare was a false alarm (Bernhard and Giegerich 2008).

iv In *Kyllo v. United States*, 533 U.S. 27 (2006), the Supreme Court held that it was a violation of reasonable expectations of privacy to use a remote thermal sensing device to measure differences in the
exterior temperature of a dwelling, and thus an unreasonable search and seizure without a warrant. In thus ruling, the Court attempted to fashion doctrine that would apply well beyond the crude sensing device employed by the police to ascertain from differential outside temperatures of the house whether Kyllo was using the high-temperature lamps to cultivate marijuana within. Justice Stevens, in dissent, argued that the case was just a garden-variety use of external observation, albeit enhanced—just like the visual observation that snow was melting differentially in areas of the home’s roof. This analysis would not apply, however to measurements obtained when someone is outside of the home. Also worthy of note, the new International Health Regulations specifically exclude thermal imaging from the definition of invasive procedure (International Health Regulations, art. 1 (definitions)).