Emergency Management for Information Systems in Public Health
A Case Study of the 2009 Pandemic-Flu Response in Japan

Tomoki MUROTA
Graduate School of Frontier Sciences
University of Tokyo/WIDE Project
Tokyo, Japan
murota@yayoi.wide.ad.jp

Akira KATO
Graduate School of Media Design
Keio University/WIDE Project
Kanagawa, Japan
kato@wide.ad.jp

Takashi OKUMURA
Center for Information Research and Library
National Institute of Public Health
Saitama, Japan
taka@niph.go.jp

***Abstract*—To appropriately respond to emergent diseases, public health authorities must make a variety of decisions, under time and resource constraints. To this end, there have been information systems in the public health sector, for its decision support. Nevertheless, during the Swine-flu outbreak in Japan, the national surveillance system did not perform well enough, in the actual emergency situations. This paper presents the case of the 2009 pandemic-flu response in Japan, and clarifies the requirements for information systems in the public health sector, with respect to emergency management. The case study suggested the following lessons. First, information systems in public health domain must possess enough flexibility to accommodate additional surveys and features to dynamically modify the existing ones, to address exceptional situations. Secondly, virtualization technologies can be a solution for flexible management of system resources in emergency situations. Lastly, we found that the actual challenge lies in the number of parties involved, including public health authorities, medical institutions, care providers, and patients, which count up to millions, or billions, suggesting the needs for *pervasive computing*, as a reasonable course to take in the domain.**

***Keywords*-Swine-flu outbreak, Decision Making in Public Health, Epidemiological Surveillance**

I. Introduction

Precise and timely information is essential to decision making in emergency management. Public health emergencies, such as bio-terrorism and pandemic outbreaks, are illustrative cases; it is critical to quickly survey the situation and to focus on crucial issues, so that appropriate responses can be made to the unknown threats. Accordingly, public health authorities are required to survey the spread of affected patients, the biological characteristics of the infectious agents, the status of medical resources in the region, such as detoxicant stock and specific medical devices, and sometimes, detailed information of each patient. Because of the nature of the problem domain, delays and misinterpretation could result in severe economic damage, or even disastrous increases in the death rate. It is clear that emergency management is an indispensable factor for information systems in the public health sector.

Indeed, due to the worldwide prevalence of the 2009 Swine-flu virus, emergency management of information systems has become a central issue for public health officials in Japan. In this country, public health authorities have been stocking therapeutic medicine and preventive equipment as a precaution against the expected pandemic Avian-flu, coupled with necessary action plans and surveillance systems. Consequently, the Ministry of Health, Labor and Welfare (MHLW) started the emergency operation, according to the predefined pandemic-flu response program, immediately after the first report made by CDC (Center for Disease Control) of the United States in late April 2009.

Owing to the insularity of the country, the epidemic curve was kept to a minimum during the initial phase, in mid-May. But, in June, a change occurred when the number of infected patients started to gradually increase. In this process of actual pandemic-flu outbreak, national surveillance systems revealed various unexpected problems, as described later in the text, and they failed to collect and analyze pandemic information in a timely and accurate manner. It was surprising that information systems for crisis control did not function well, even though Japan is known as one of the most high-tech countries in the world, possessing high-speed communication networks across the country, and with millions of the latest computers in its offices. This paper is a case study of public health information systems under such an emergency situation, and focuses on why the systems did not work and how the authors reacted as information system researchers (Note that the last author is an M.D., Ph.D. in Computer Science).

The paper is organized as follows. First, we overview the pandemic outbreak of Swine-flu Virus in Japan 2009, followed by a description of the epidemic surveillance system and its operation during the Swine-flu outbreak, clarifying the problems encountered. In section IV, we describe our response to the situation; indeed, for the emergency response, we were forced to develop another surveillance system in a very short time period, using the Iterative and Incremental Development (IID) approach. Section V is a discussion section, where we discuss emergency management for public health information systems, emphasizing the contributions of pervasive computing in this domain. Section VI summarizes highly related work, and the last section concludes the paper.

II. Swine-Flu Outbreak 2009 and Public Health Authority in Japan

This section overviews the ongoing public health crisis in the world, the Swine-flu pandemic in 2009. The series of worldwide events first began in the United States CDC, when they reported the new H1N1 influenza virus, on April 23. On the next day, World Health Organization (WHO) announced the emergence of new influenza spreading in Mexico and in the United States.

Right after the announcements, MHLW set up a headquarters for the pandemic-flu response in Japan, according to the action plan prepared for the Avian-flu outbreak. On April 28, WHO raised the pandemic alert to Phase 4, and on April 30, they raised it to Phase 5, which indicates continuous human-to-human infection in a region and alerts the authorities of a worldwide pandemic. Accordingly, MHLW reinforced the quarantine officers at major airports, particularly for passengers on North American flights, to detect and isolate febrile patients. This was known as a "shoreline operation", and quarantine tried to prevent the inflow of the new influenza virus into Japan. MHLW also performed other possible measures, coordinating with international authorities, neighboring countries, other ministries, regional governments, local medical institutions, schools, and so on, while reinforcing the headquarters.

However, the index case of the H1N1 Flu was finally found on May 16, in the western Japan area. Surprisingly, the case did not have a history of international travel, and the infection route was not traceable. This indicated that the virus was already prevalent in the region, and in fact, the number of patients rapidly expanded in western Japan, right after the discovery of the index case. This trend once subsided in late May, but, in mid-June, it changed to an upturn again, and the number of confirmed cases reached a thousand, on June 25.

In the initial phase of the domestic outbreak, it was possible to examine and trace all the suspects, sampling specimen for confirmation of the virus DNA. However, as the number of patients increases, it gradually became impossible for public health officials available in each region to locate and trace all the specimens and the patients. Consequently, MHLW abandoned the thorough investigation policy, on June 19, switching to a looser policy, to count only the cluster incidences and to monitor the biological characteristics of the virus. The primal goal was also changed to mitigate the infection rate, in the aiming to protect the care providers from being overloaded by the outbreak patients.

III. Surveillance Systems Under Pandemic-Flu

To support the public health services in the country, MHLW has been operating the epidemic surveillance system with National Institute of Infectious Diseases (NIID), named the National Epidemiological Surveillance of Infectious Disease (NESID). The system is a nationwide surveillance system of infectious diseases, which connects sentinel medical institutions, regional public health centers, public health sections of prefectural/metropolitan governments, and the ministry. In a regular state, sentinel institutions report weekly summaries of monitored infectious diseases such as influenza, rubella, and mumps, and such information is automatically aggregated and analyzed by the system for geographical mapping.

Although the listed agents, such as influenza and rubella, are moderately mild, there are a variety of infectious diseases, which are sometimes lethal, such as Ebola hemorrhagic fever, yellow fever, and smallpox. To manage the public health emergencies caused by such agents, the system has an emergency features to safely where the patients' information among medical institutions, public health centers, public health sections of local governments, and MHLW. In addition to the secured exchange of privacy information, the system has been designed with flexibility to accommodate new surveillance, for emergent infectious diseases.

Although these features were provided for emergency management, the situation caused by the unforeseen virus was beyond the the architect's imagination. For example, because there was no sufficient information about the nature of the emergent disease, the headquarters was forced to collect detailed background, symptoms, clinical conditions, and infection routes of each patient. However, comment fields for additional information in the patient database turned out to be insufficient, because the headquarters required far more detailed information, particularly for high-risk inpatients. It was also found that significant time and cost were necessary, to modify the database, mostly due to the governmental business practice of competitive bidding. Furthermore, in such an outbreak, regional public health centers were overwhelmed by the liaison with patients, medical institutions, and local governments. They became exhausted by the routine tasks for their residents, and they were unable to operate the surveillance terminals for detailed case reports.

Another challenge was how to accommodate frequent changes of the surveillance policies caused by the phase transitions. For example, in the early stage of the outbreak, the headquarters tried to specify the location of all patients and suspects. Then, the policy was changed to detect cluster incidences, requiring at least one specimen per cluster to confirm the diagnosis by the virus DNA. Finally, after actual outbreaks occurred throughout the country, the headquarters suspended the confirmation policy, because the number of patients surpassed the capacity of the local authorities and the examination facilities. For each phase, the headquarters needed to modify the surveillance design, and thus, the surveillance system was required to flexibly adapt to the new schemes and policies.

Figure 1-Left shows the data flow in the actual operation at an early stage. There were 180 thousand medical institu-

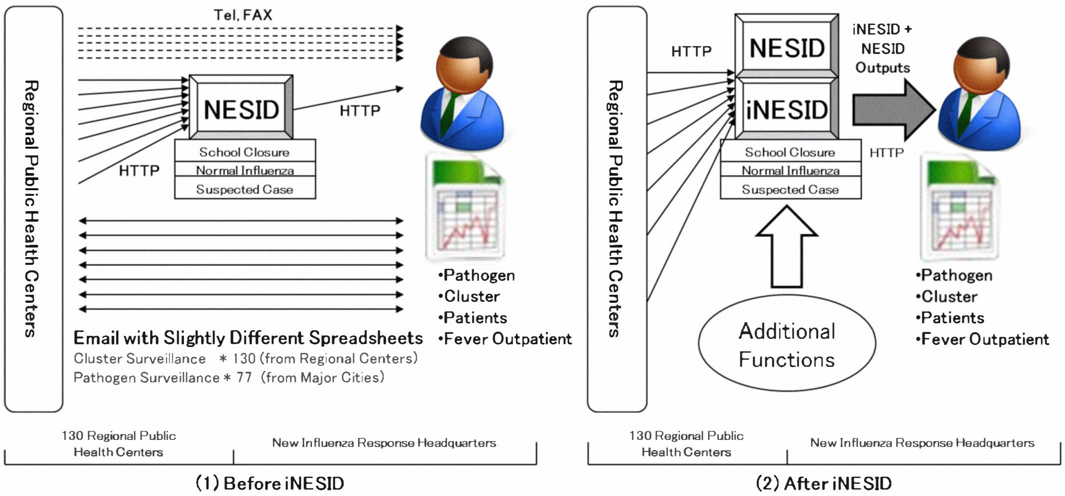

Figure 1. (Left) This is a data flow of the information for the pandemic-influenza response. Medical institutions report patient information to regional public health centers. Next, the public health centers report outline information to the local government. However, because the surveillance system was unable to accommodate the necessary surveys for the 2009 pandemic-flu, the headquarters distributed spreadsheet files to the reporting sections, and ordered them to send back the files as email attachments. Because of the variety of the report templates versions, local governments were overloaded and the headquarters was overwhelmed by the number of reports, resulting in considerable inefficiency. (Right) The figure suggests that the iNESID system greatly simplifies the data flow.

tions in Japan which potentially examined the pandemic flu patients (not shown). These institutions are supervised by 510 public health centers throughout the country, which are subsidiary to the local governments. Public health sections of the local governments are obliged to report their summary information to the government headquarters in a timely manner. And because the surveillance system was not flexible enough, the headquarters created spreadsheet files for each survey, and ordered public health sections to submit the files as email attachments for each week.

As the figure suggests, the scheme was considerably inefficient in nature. Local governments were forced to update and manage the versions of the report templates on their own, and they sometimes used obsolete templates and misinterpreted the fields in the files. Headquarters was required to keep track of the submissions from many sections, and they had to manually aggregate the submitted files, potentially leading to human errors. To improve the situation, it the authors started a project to improve the surveillance system.

IV. Agile Development of a National Surveillance System

Because actual operation of the NESID system was outsourced to a system integrator company, we did not have access to the running system, to analyze and modify the existing surveillance. Accordingly, we planned to develop another surveillance system, hoping to merge the two systems in the near future. Because of the intention, we named this system "interim NESID" system (iNESID). As illustrated, iNESID totally substitutes the email-based communication, while allowing flexible modifications of existing surveys and addition of new surveys, connecting regional public health authorities and headquarters (Figure 1-Right).

For the development of the iNESID system, we adopted the "Iterative and Incremental Development (IID)" approach [1], also known as "agile" development. It is a development paradigm, actively investigated in Software Engineering field, where a system is developed through iterations of short-term development cycles. In this approach, each iteration is driven by demonstration and user feedback, and this presents a striking contrast with the "waterfall" approach, where demonstration is performed in the final phase of the development. Advocates say that the short development cycles can avoid mismatches between user needs and the actual products, which sometimes happen with the traditional approach. The advocates sometimes further claim the advantage of the IID approach, in respect to cost, time, and product quality.

Figure 2 shows the development process of the iNESID system. In this development, headquarters decided to develop the iNESID system on July 3, 2009 (Day 1). We started development on Day 2, with the LAMR (Linux, Apache, MySQL and Ruby) setting, and "Ruby on Rails" framework [2], [3] for the agile development. We also managed to set up the necessary servers, and to arrange the necessary network connectivity. The prototype was ready by Day 4, which included user authentication and simple report forms for the surveillance. Based on the feedback, we implemented administrative functionality, such as "surveillance news", in the next timebox, followed by another demo on Day 8. Adjustments were made for the GUI design, e.g. warning to wrong inputs, and further functionalities were implemented, such as file exporting. We finalized

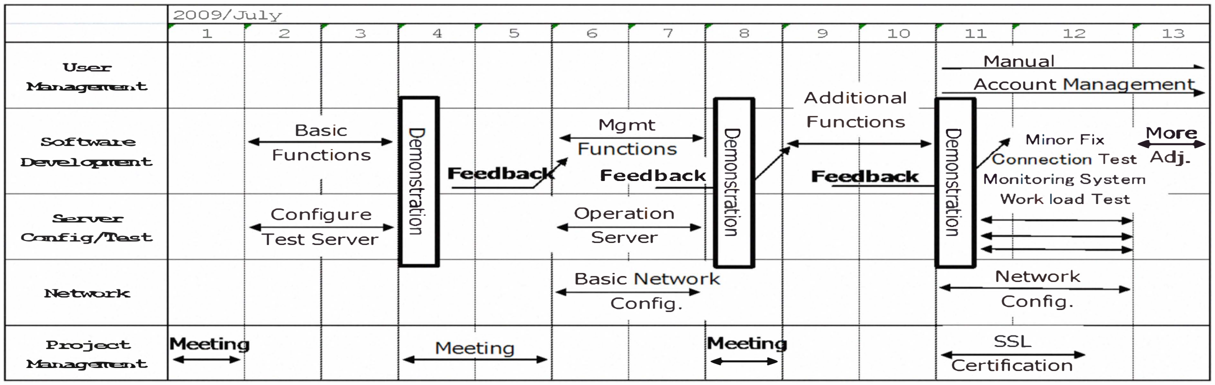

Figure 2. Development processes of iNESID system. It comprises three iterations of two-day timebox, each with demonstration.

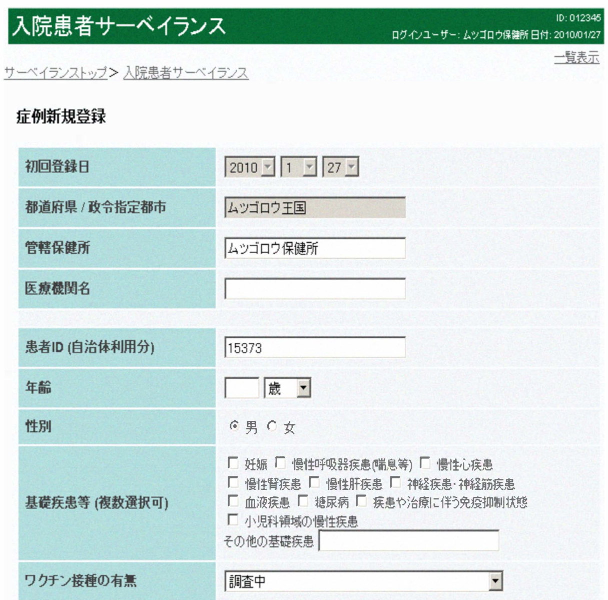

Figure 3. This is an input form of iNESID system (in Japanese). Users can input the following patient's data: Standard demographics (age, gender), important dates (date of onset, date of hospital admission), clinical presentations, past medical history (including pregnancy) and complications. These conditions might influence the severity of infection, and alert the authorities.

the development with stress testing, connectivity testing and performance tuning. By Day 13, the iNESID system was almost ready to be served to public health authorities throughout the country.

Figure 3 and Figure 4 show sample snapshots of a patient form and a cluster report form, respectively. Utilizing these forms, public health sections of regional governments submit case summaries and their weekly reports. For privacy concern, we used SSL connections and forced reporters not to include any privacy information, such as name and exact date of birth.

Now, it is easy to see that the cost for submission management by the local authorities can be substantially reduced by the Web-based system, and the data is automatically shared

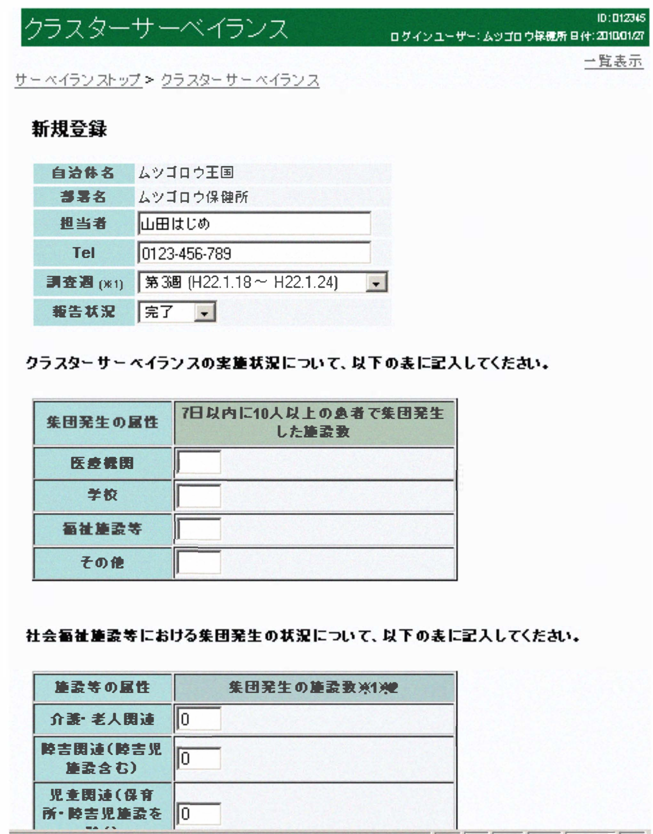

Figure 4. This is a report of a cluster surveillance in iNESID system, summarizing the number of affected clusters for each category, such as clinics, schools, and nursing homes (in Japanese). Public health centers submit the reports weekly via the system.

among the local government and the ministry, leading to improvement of the quality and the cost of the surveillance (see also Figure 1-Right). However, because patient data occurs at medical institutions, there was still great inefficiency on the regional governments' side, where the government officials manually inputs the necessary data to the Web-based system, reported by the medical institutions via faxes and phone calls. Indeed, it is where the real challenge lies, because the management cost would be prohibitive, to allow all the medical institutions and clinics in the country to submit the reports to the on-line system.

V. Discussion - Emergency Management for Information Systems in Public Health

The case study teaches several lessons for governmental decision support systems, particularly for emergency management. Because emergencies might bring about unexpected and dynamically changing situations, systems must possess sufficient flexibility in terms of hardware, middleware, application and deployment.

First of all, the system should have sufficient headroom for additional hardware, coupled with stable and secure network connections. Even though the system might possess redundant servers for fault tolerance and disaster recovery, an emergency might necessitate additional servers to cope with unexpected events, as we confronted. For this reason, it would be preferable to have a flexible resource pool, which contains server resources and extra network connectivity, coupled with excess storage. IaaS (Infrastructure as a Service) approach, which is virtualization of hosts, disks, switches, and routers, can be a reasonable option here, so as not to waste the reserve resource in peacetime. A more elaborate solution, targeted for higher system availability [4], might fit as well here.

Second, the emergency management system should have middleware service, which supports user management and access control. The system has to provide an easy way to quickly setup systems, including commodity operating systems and commodity database management systems, on the virtualized hardware. In fact, for the rapid development of the surveillance system, we consumed most of out time in this phase; user management and access control. In this regard, commercial services have already been providing such a feature, as PaaS (Platform as a Service). For example, Google App Engine and Amazon EC2/S3 are offering such functionalities for commercial services, and such a model can also be applied to emergency response.

The third issue concerns the application layer, particularly regarding the agile development for emergency management. As we illustrated in the case study, it would hardly be possible to completely forecast the emergency situations. Accordingly, the decision support systems should allow flexible modifications of existing services and accommodations of new functionalities. To this end, there are two contrastive approaches. One approach is to set up a new system, as we tried with this project. The other extreme is an authoring system, like Google Docs (Figure 5) and Filemaker [5]. These systems allow administrators to flexibly develop web services without any programming knowledge. Because these options are not exclusive, the best option would be to support both approaches, if a sufficient budget is available and security levels are equal. Note that most governments

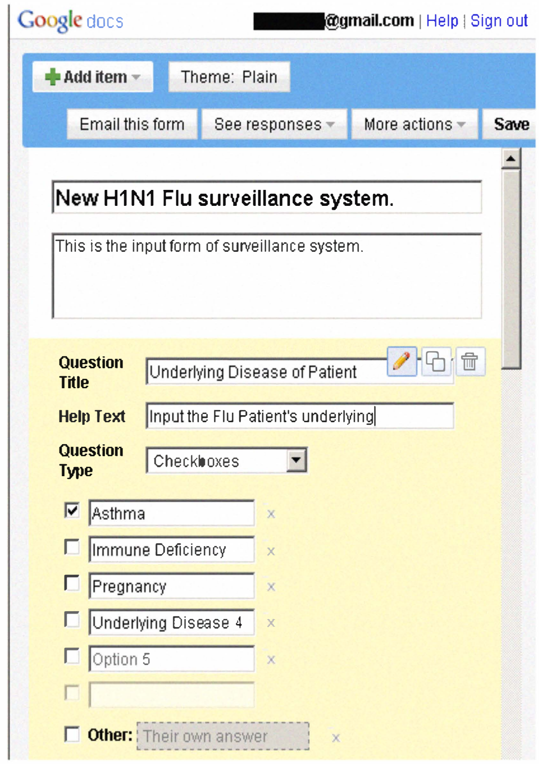

Figure 5. Prototype input form of Google Docs can be created with a GUI, similar to word-processors. Created forms are hosted on the Google servers and accessible through the Internet. Administrators can easily manage the collected data with a web-based spreadsheet interface.

have their own security and privacy policies, which could be too strict to use the cloud service in the private sector.

Lastly, after all the development processes, there is another phase for deployment and actual operation. As illustrated in the last section, Japanese medical care system comprises thousands of medical institutions, supervised by hundreds of public health authorities. Accordingly, decision support systems in the public health sector must address the scalability issue for deployment and operation. Indeed, this is the most challenging part of the story, because deviation of operator skills increases as the number of users increases, and human factor would become dominant in the entire cost. Accordingly, it would be reasonable to exclude the human factor in the data acquisition phase, originating 180 thousands medical institutions, or even the entire population. In this regard, more and more hospitals are now installing electronic medical record (EMR) systems, and it is too natural to pervasively connect the EMRs for automatic data gathering. The challenge is that the data collection must be scalable, and the network must be made hierarchically and pervasively, though it is left for our future work.

VI. Related Work

The National Retail Data Monitor (NRDM) [6], [7] is a surveillance system designed and operated by the University of Pittsburgh. One significance of the system is that it connects retail stores in Pennsylvania to monitor the sales of over-the-counter (OTC) drugs, which is a simple indicator of a disease outbreak. Another advantage is that the system connects information systems in major hospitals, which upload the data of anonymized patient visits. Because of the automated process, the system can efficiently monitor biomedical hazards in the region. A drawback is the inflexibility of the surveillance, because the data flow is hardcoded in the systems.

There is another challenging system in the United States. The Google Flu Trends [8] is a nationwide surveillance system, which is so unique in that it has no direct relation to any existing medical care system. Instead of gathering data from medical institutions, the system utilizes Internet search trends to monitor the prevalence of infectious agents. This is based on an assumption that there is a correlation between search words in their service and prevalence in the region inferred from the user's access profile. This unique approach is advantageous in that it efficiently scales and minimizes report latency. The downside is that the system is not resistant to rumors, which could be alleviated by rumor detection [9].

In Europe, there is a surveillance system to correlate Internet news and multiple sources of electronic medical information [10]. This system analyzes information on daily news, and automatically generates necessary alerts. In the United Kingdom, there is a surveillance system, based on a large-scale telephone triage service by the National Health Service (NHS) [11]. This system analyzes the patients' age, address, and condition, to reveal certain tendencies.

In Japan, there have been several systems for outbreak surveillance. The National Institute of Infectious Diseases is operating the NESID system, with the Ministry of Health, Labor and Welfare. They also operate another surveillance system, for patient symptoms [12]. The Ministry of Education, Culture, Sports, Science, and Technology (MEXT) is also monitoring elementary and high schools for their school or class closure by contagious agents. In the private sector, there is a surveillance system by volunteer pediatricians, to detect the outbreak of common agents [13].

VII. Concluding Remarks

To appropriately respond to unknown threats to the public health, public health authorities must make a variety of decisions under time and resource constraints. Because of the nature of the systems, outbreak surveillance systems are designed with some flexibility. Nevertheless, our case study illustrated that, in actual emergency situations, unexpected events could emerge, which might necessitate exceptional operations. To accommodate the exceptions, public health information systems must possess further flexibility to rapidly modify and develop surveys as a means for emergency management. In this regard, most of the issues can be addressed by virtualization technology, which can pool excess system resources without wasting capacity, while realizing easy installation of new systems. However, particularly for public health systems, the real challenge is in the number of authorities, medical institutions, and healthcare providers, which number millions, and thus, pervasive computing possibly with direct data gathering from EMR would be a reasonable course to take in the domain, although the verification is left for future work.

References

[1] C. Larman, *Agile and Iterative Development.* Addison-Wesley, 2003.

[2] M. Bachle and P. Kirchberg, "Ruby on Rails," *IEEE Software*, vol. 24, no. 6, pp. 105–108, 2007.

[3] D. Thomas, D. Hansson, L. Breedt, M. Clark, T. Fuchs, and A. Schwarz, *Agile Web Development With Rails.* Pragmatic Bookshelf, 2006.

[4] N. Bartolini, G. Bongiovanni, and S. Silvestri, "Distributed server selection and admission control in replicated web systems," in *Proc.* IEEE *ISPDC'2007*, Washington, DC, 2007, pp. 221–228.

[5] FileMaker, Inc. (2009) The Database Software FileMaker website. [Online]. Available: http://www.filemaker.com/

[6] K. J. Henning, "Overview of syndromic surveillance what is syndromic surveillance?" Morbidity and Mortality Weekly Report (MMWR), CDC, Tech. Rep. 53(Suppl);5-11, Sep, 2004.

[7] T. Wu, F. Shih, M. Yen, J. Wu, S. Lu, K. Chang, C. Hsiung, J. Chou, Y. Chu, H. Chang, C. Chiu, F. Tsui, M. Wagner, I. Su, and C. King, "Establishing a nationwide emergency department-based syndromic surveillance system for better public health responses in taiwan," *BMC Public Health*, vol. 8, pp. 8–18, Jan 2008.

[8] Google Inc. (2008) The Google Flu Trends website. [Online]. Available: http://www.google.org/about/flutrends/how.html

[9] S. Reece, A. Rogers, S. Roberts, and N. R. Jennings, "Rumours and reputation: evaluating multi-dimensional trust within a decentralized reputation system," in *in Proc. ACM the 6th international joint conference on Autonomous agents and multiagent systems (AAMAS'07)*, New York, NY, USA, Jan 2007, pp. 1–8.

[10] J. Linge, R. Steinberger, T. Weber, R. Yangarber, E. v. d. Goot, D. A. Khudhairy, and N. Stilianakis, "Internet surveillance systems for early alerting of health threats," Eurosurveillance, Tech. Rep. 2009;14(13)2, Apr, 2009.

[11] G. Smith, D. Cooper, P. Loveridge, F. Chinemana, E. Gerard, and N. Verlander, "A national syndromic surveillance system for england and wales using calls to a telephone helpline," Eurosurveillance, Tech. Rep. 2006;11(12), Dec, 2006.

[12] T. Sugawara, Y. Ohkusa, M. Shigematsu, K. Taniguchi, A. Murata, and N. Okabe, "An experimental study for syndromic surveillance using OTC sales (in japanese)," *the journal of the Japanese Association for Infectious Diseases*, vol. 81, no. 3, pp. 235–241, 2007.

[13] The ML-Influenza Database Project. (2009) The ML-Infurueza Epidemic Frontline Information Database website. [Online]. Available: http://ml-flu.children.jp/