Chapter 12
Biosurveillance and Dentistry

Miguel H. Torres-Urquidy

12.1 Dentistry and Modern Public Health Surveillance

The public health environment (like the rest of healthcare) is changing and incorporating digital strategies at the forefront of their responses to public health events and routine public health interventions. The H1N1 pandemic, SARS, Ebola epidemic, and Zika pandemic are recent global events of public health concern (Fineberg 2014; Dixon et al. 2014; Fauci and Morens 2016). In addition, other local crises such as the US opioid epidemic (US Department of Health and Human Services 2017), have reinforced the need to establish bidirectional communications between clinical practices and public health authorities. As a result, organized healthcare has established and adopted protocols to rapidly handle patients and related risks adequately. It is now common in clinical practices to hear the question "have you travelled abroad recently?" or "have you been to places experiencing a public health emergency?" Furthermore, guidance from public health authorities can be seen posted throughout halls or clinical spaces in practices. These messages and warnings are now also part of electronic health records and patients are questioned and treated accordingly. Public health authorities (federal, state, and local) continue to develop strategies to reach both clinicians and the general public and having the capacity to handle electronic health record data is a high priority for all of them.

In the case of surveillance, there are a myriad of mechanisms to collect, distribute, and aggregate information (Groseclose and Buckeridge 2017). In addition, in the US, the public health surveillance effort is highly distributed where, depending on the type of condition, funding stream, and/or regulation, the authority and scope of responsibility of the different public health agencies is spread across geographical boundaries. Furthermore, local, state, and/or federal priorities can modify the way surveillance gets conducted. Whether responding to public health emergencies,

M. H. Torres-Urquidy
Centers for Disease Control and Prevention, Atlanta, GA, USA
e-mail: miguel@forwardthinkingconcepts.org

A. Acharya et al. (eds.), *Integration of Medical and Dental Care and Patient Data*,
Health Informatics, https://doi.org/10.1007/978-3-319-98298-4_12

adjusting to local geographic conditions or events (e.g. hurricanes) or new evidence, requires public health surveillance efforts to remain flexible.

Another trend that is important to recognize is how evidence is gathered, synthesized, and made available. Big Data, cloud, and edge (mobile) computing are enabling more organizations to develop their own public health insights (Griebel et al. 2015). Large hospital systems, data consortiums, and public health partnerships are empowering the academic community, health insurance companies, and employers to design and implement their own public health interventions. In summary, population health (Kindig and Stoddart 2003) is steadily solidifying and expanding the number of those who are part of the public health system.

In this chapter, we focus on the response efforts to bioterrorism and, although such a term is less in vogue nowadays, it is a constant element of worry among public health planners. It is also important given that systems and mechanisms put in place to identify, prevent, and respond to such bioterrorism events are likely to be used in many other public health situations. This is not to take away from other traditional public health surveillance approaches and very successful interventions (such as national surveys and water fluoridation), yet in the case of dentistry and biosurveillance, there is plenty of room to grow and integrate.

12.2 Dentistry and Bioterrorism

During March 27 and 28 of 2003, the American Dental Association and the US Public Health Service sponsored the conference "Dentistry's Role in Responding to Bioterrorism and Other Catastrophic Events" (Palmer 2003; National Institute of Dental and Craniofacial Research, 2004). This meeting reviewed several aspects of bioterrorism and the dental profession: the nature of biological pathogens and its oral manifestations, what needed to be communicated, how dentists should participate, etc. Dr. Michael C. Alfano described the difficulties that biological pathogens create for clinicians because "they are so insidious." While discussing the anthrax mailings after September 11th he pointed out that: "… early symptoms appeared so they resembled the aches, fever, and malaise of flu so those affected delayed seeking treatment, a delay that has proven fatal in some cases". Lieutenant Colonel Ross H. Pastel of the US Army Medical Research Institute of Infectious Disease (USAMRIID) listed the "Category A" pathogens as defined by the Centers for Disease Control and Prevention, and those are: smallpox, anthrax, plague, botulinum toxin, tularemia, and viral hemorrhagic fever. He also described an outbreak of smallpox in Yugoslavia in 1972 and the measures that had to be taken to control it. Dr. Michael Glick described the oral manifestations of smallpox showing "signs 24 h before skin rash. These oral signs include tongue swelling, multiple mucosa vesicles, ulceration, and mucosal hemorrhaging. Oral signs are also evident in inhalation and gastro-intestinal anthrax. In oropharyngeal anthrax the mucosa appears edematous and congested; there may be neck swelling, fever, and sore throat".

Dr. Ed Thompson, at the time Deputy Director of the Centers for Disease Control and Prevention, mentioned that "None of the new counter-bioterrorism measures can be effective unless local health practitioners are vigilant in observing and reporting a possible disease outbreak. Such surveillance—knowing what to look for and whom to report to—is critical and applies not only to suspected bioterrorist agents, but to a list of reportable diseases which has grown to include such entities as West Nile virus and Severe Acute Respiratory Syndrome (SARS)." Dr. Sigurs O. Krolls presented the response at the local level and he "stressed the importance of communication and the need for redundant systems", "to keep all the parties informed". He also posed the question "Can dentists recognize signs and systems of contagious diseases?", and emphasized that education is essential. Dr. Louis DePaola made several recommendations that can be key in the scope of this paper by saying "dentists can contribute to bioterrorism surveillance by being alert to clues that might indicate a bioterrorism attack. Such surveillance would note if there is an influx of people seeking medical attention with non-traumatic conditions and flu-like or possibly neurological or paralytic symptoms… or even specific signs of a bioterrorist agent. Patterns of school or work absence, appointment cancellations or failures to appear, could also be indicators." Dr. DePaola made clear that in cases of limited release of bioterrorist agents, dentists "have little to offer" but "a widespread attack can certainly tap into dental professional skills in recognition, isolation and management". In addition, Dr. Guay (Guay 2002) lists all the possible roles in which dentists can participate including "education, risk communication, diagnosis, surveillance and notification, treatment, distribution of medications, decontamination, sample collection and forensic dentistry."

These recommendations provide initial knowledge that can drive the development of integrated health records. It is also important to understand that integration needs to occur within existing technologies such as electronic dental records (EDR), previously called the computer-based oral health record and respective electronic health standards. The final recommendation from the meeting stated that to play an important role in biodefense a serious amount of coordination and preparation will be required, not only from dentists but from other groups, most likely requiring medical and dental data integration.

12.3 The Computer-Based Oral Health Record (COHR) and Computer Ownership

The COHR, as described by Rhodes (1996), "can provide a structure for documentation that goes beyond the concept of a blank form on a page, it includes a glossary of dental terminology for the entire content of the form as well as knowledge bases and expert systems that can enhance the practitioner's diagnostic and treatment planning decisions". He also acknowledges that one of the advantages of this type of documentation is that it "is much more transportable". He also recognizes the

need for standardized methods for collecting information from dentists. Schleyer and Eisner (1997) defined several scenarios where the COHR is used in a "shared" environment where several healthcare providers interact and information is seamlessly communicated, improving the decisions made by clinicians. Delrose and Steinberg (2000) discuss how the "Digital Patient Record" enhances clinical practice by providing "better quality information" to the clinician. Although all of these benefits sound promising and encouraging some still express concern about the lack of standards among different information systems, which translates into communication breakdowns (Schleyer 2003). On the other hand, Heid et al. (2002) list all the steps that are currently being taken by different organizations such as the ADA in order to produce a standardized COHR. Other examples of standardization can be found in a paper presented by Narcisi (1996) where ADA's participation as a voting member in the American National Standards Institute has allowed EDI or the COHR to be discussed and improved at a national level, now much commonly known as the Electronic Dental Record or EDR.

Additional influences in the standardization of the EDR are the security regulations mandated by HIPAA, the Health Insurance Portability and Accountability Act of 1996. Dentists are required to "adopt practices necessary for compliance" (Sfikas 2003; Chasteen et al. 2003). These and other regulations (Szekely et al. 1996) will encourage homogeny among different system vendors. Computer ownership, on the other hand, has increased steadily during the last 25 years. According to Schleyer et al. (2003) in 1976 only 1% of dental professionals used computers in their practices compared to 85% in 2000. Additionally, similar trends in Internet connectivity where described. Acharya et al. (2017) reported that chairside Internet utilization increased to 72% in 2017.

12.4 Dentists, Source of Information for Detecting Biosurveillance Events

Given the previous background (levels of adoption/utilization) it is plausible to consider using EDRs as a monitoring source for public health events. Next, we present a blueprint for developing a biosurveillance system.

12.5 Proposed Approach

The purpose of developing an electronic health surveillance system is to gather information from patients directly (Wagner et al. 2006) by detecting signs and/or symptoms, or indirectly by obtaining other types of information such as over-the-counter medication sales, patients' no-shows, usage of Internet search engines, keywords, etc. In this particular case, the proximity of contact between

the dentist and the patient is equivalent to a medical inspection in terms of immediacy and/or closeness. Such signs and symptoms can be easily detected if the dentist is properly prompted to search for them. This is just one example of how a system could provide assistance in the detection of a bioterrorism incident.

But, before describing our proposed approach, it would be important to describe the principles behind biosurveillance systems including those such as syndromic surveillance as well as the technical aspects behind them (Tsui et al. 2003). As an example, we describe the Realtime Outbreak Disease Surveillance Laboratory (RODS Lab). RODS Lab uses data obtained directly from chief complaints in the emergency departments of hospitals to construct time series and other forms of aggregated data, to characterize the health status of a specific population. These aggregated data are then assessed by detection algorithms, which can issue alerts in case patterns in the data suggest the emergence of a bioterrorism event.

When implementing such systems, it is important to take into consideration the scale and number of possible contributors. Traditional biosurveillance systems use information collected from hospitals and/or health systems. In the case of large implementations, with dissimilar technologies, careful consideration needs to occur to manage and integrate different kinds of data sources, in our example, EDRs. With this in mind, we proposed a set of elements for creating a biosurveillance system based on EDR data.

The proposed approach should work at multiple levels:

- Communications: The system would have to provide a mechanism to alert the dentist if there is suspicion that a bioterrorist attack may be happening. The mechanism would increase the dentist's awareness in case of finding suspicious signs or symptoms in a patient. This can be triggered by the patient's characteristics such as geographic location of residence, etc.
- Surveillance: Automated collection of information from the patient's EDR. The system would report to a central database, signs or symptoms of interest. The aggregation of this data could generate information that would eventually detect the presence of patterns that may lead to the early detection of such events.
- Reuse of data: Collection of additional information, which combined with other sources, can be useful in terms of detecting or tracing some incident. Patient "no-shows" is the primary example, that, if combined with others such as work or school absenteeism can provide a relevant pattern for public health officials.

12.6 Use Case Example

Dr. X, who practices in a community 20 min away from Capitol City, installed a new clinical management system 2 months ago. Among the features that were included in this new clinical management system (CMS), a bioterrorism detection module was added. She felt curious because of recent news she read in the newspaper about possible attacks against the US and decided to install the feature. She read

about how the module would work in combination with the CMS she just bought. The educational information provided with the software instructed Dr. X, that in case a patient victim of a bioterrorism attack happens to be seen in her practice, the software would collect information and would send it to public health officials. When installing the software, Dr. X was asked if she agreed to share such information with public health authorities and she approved.

During the week, a patient walked into Dr. X's dental office. The patient presented some signs that indicated the presence of a disease of unclear origin. An epidemiologic study later would show that the patient was present at a football stadium when an infectious agent was released (Fig. 12.1). Although, at that time his medical history showed no indication of a systemic disease, the presence of multiple *oral vesicles* prompted the dentist to make an annotation into the COHR. The system, by using a natural language processing engine, detected the sign and sent this information to a central database. The patient was discharged and instructed to take some support medication to treat the oral ulcers. The next day, the central database pinpointed the presence of an out of the ordinary increase in the number of cases with the same signs and symptoms around that region. When the presence of this peak was detected, the central server sent a request to the dentist's computer for additional information. One of the requested elements was if there was any use of medication for treating oral ulcers. Fortunately, this information was available. The central database crossed this with the information of other surveillance systems together with the information from other patients that happened to have similar clinical signs and/or symptoms. Dr. X received an email from a public health official asking her to communicate to the local health department to discuss information about one her patients.

The case depicted above simulates the release of smallpox during a football game. In the case of smallpox, oral symptoms include tongue swelling, multiple oral mucosal vesicles, ulceration, and mucosal hemorrhaging (National Institute of

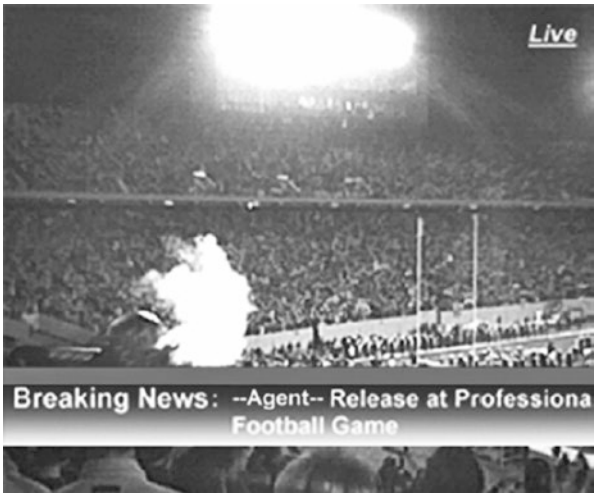

Fig. 12.1 Biosurveillance systems should be cognizant of different kinds of events since this can be linked to issues of public health concern

Dental and Craniofacial Research 2004). Dentists could be alerted by an electronic system to search for such signs or they can be detected automatically. In case of a high incidence within a group of patients, in a confined area, public health officials get to be notified.

In our hypothetical case there are issues that need to be addressed in order to make such a detection system feasible:

12.7 System Design

As described by Schleyer et al. (2006) and Acharya et al. (2017), 85% of dentists in the US use a computer in their practices. Given the current number of dentists in the US, this figure would generate an estimate of 166,000 computers in dental practices, all possibly eligible to be public health surveillance data sources.

Ideally, a biosurveillance system would rely on existing EDRs already implemented by practices. Currently there are many clinical management software packages in the dental market (Toth 2015). It is possible to create modular software that would interact with the practice management system, and allow for "querying" for specific clinical data. Additionally, a natural language processing engine could be embedded into the application in order to detect variations of data input in the EDR. Nevertheless, it is necessary to obtain a detailed list of the oral manifestations of diseases that are likely to be found in patients. Successful implementations of similar systems have been shown to work successfully (Chapman et al. 2001; Ivanov et al. 2002), and using the same approach for our system seems technically feasible.

This collected information later would be sent to a central server in order to be analyzed and interpreted.

12.8 Software Architecture

The components of our system would be as follows (Fig. 12.2):

- Thin client: a software application distributed for data collection. It would be conformed of a "querying" mechanism, combined with a natural language processing engine and a communication module. This software client should be as thin as possible to reduce the workload on the dentist's equipment and should be embedded as a plug-in for current clinical management systems. Vendors should be contacted to ask for their collaboration in the development of such an application to ensure maximum compatibility and integrity of data collection. In case the dentist uses a cloud based EDR, the "client" would collect information from the cloud service and would then resubmit the information to the central server.
- Central servers: server software in charge of integrating all the data collected from dental offices. It has to be capable of handling simultaneous requests from multiple users. This server would integrate all the data and would perform an

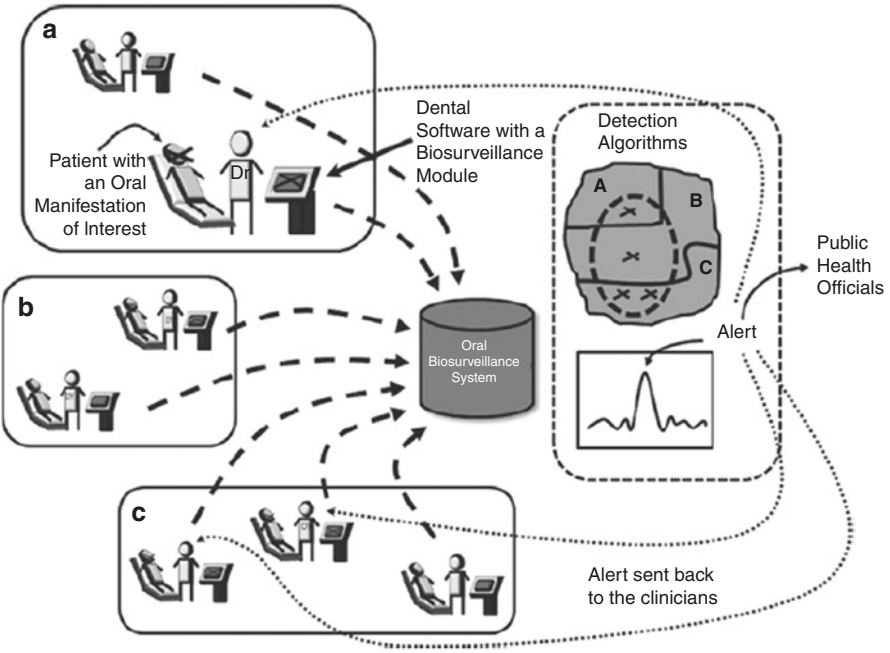

Fig. 12.2 System architecture of a biosurveillance system using information from dental practices

analysis with the intention of detecting anomalies. It would be recommended that redundant servers should be located in different data centers with mirroring capabilities to guarantee their survivability in case of technical difficulties.

- Communication network: the transmission of information should be done using the Internet. This, of course, would essentially depend on the practitioner's current connectivity. If that is not available, backup connection to the central servers should be established.

12.9 Standards

Dentistry uses several standards for transmission of health related information. Clinical management systems use standard-based technology to transmit information (Narcisi 1996; Chasteen et al. 2003; Szekely et al. 1996). As we describe elsewhere in this book, the development, implementation, and use of electronic standards among dentists is on the rise and this can expedite the implementation of a biosurveillance system. The use of standards can also open the opportunity to link EDR systems with other, already existing, public health surveillance systems.

12.10 Security and Redundancy

Information security remains a constant challenge given the constant unveiling of software and hardware vulnerabilities. As a result of this, a maintenance process should be in place to make sure that the components of the surveillance system remain secure and up-to-date. On the server side, redundancy should be provided so downtime is reduced. The system should be developed so mirrored servers are always up and running. Data integrity mechanisms should also be considered as well as other industry best practices.

12.11 Privacy and Confidentiality

Privacy and Confidentiality are important issues that need to be incorporated as part of a robust biosurveillance system and distinct regulations such as HIPAA require protecting patient information (Frist 2002; Chasteen et al. 2003; Bayer and Colgrove 2002; Etzioni 2002; Ivanov et al. 2002). In our use case we described the use of several sources of information for detecting a bioterrorist attack. We described how syndromic information, which initially should be de-identified, is transmitted to a central database. Later, after the suspicion of a bioterrorist attack, more information is requested (medications) and more inferences are made. This, although technically possible, would require allowing for sharing clinical information with public health authorities. This leads to the discussion about "individual rights" vs. "common good". Although HIPAA addresses public health (Gesteland et al. 2003; Lumpkin 2001), some other implications may arise and the health professionals including dentists, physicians, and public health officials, and patients should discuss and address such issues.

Careful consideration has to be given to which information is required to detect a bioterrorist attack, while also keeping in mind that it is always important to reduce, as much as possible, the collection and transmission of patients' information over the Internet or any other network.

12.12 Detection Algorithms and Evaluation

A detection algorithm has to be created or adapted in order to determine the presence of a bioterrorist attack. Some algorithms have proven their effectiveness (Wong et al. 2003) and it is likely that, from these, a new analysis should be done in order to select or create one that addresses the particular needs of our system.

A study was conducted to assess the feasibility of using oral manifestations in order to detect disease outbreaks (Torres-Urquidy et al. 2009). Torres-Urquidy

and colleagues found it is feasible to use oral signs and symptoms to create biosurveillance signals. In their study, the most promising signals were those for botulism and smallpox. For data extraction, the investigators used natural language processing followed by the use of statistical methods such as moving average (MA) to serve as part of a detection algorithm.

The system should also be thoroughly evaluated, before and after implementation. Evaluation prior to implementation can be performed using simulated data. Simulation and modeling techniques (Reshetin and Regens 2003) have been used to estimate the effects of a bioterrorist attack. The same techniques can be used to evaluate our system. In the study by Torres-Urquidy et al. (2009), the investigators utilized synthetic outbreaks to test the performance of different signals. From their evaluation process, they learned, for instance, how many cases would be necessary to occur for the system to reach certain detection thresholds.

12.13 Dissemination and Collaboration

Several dental organizations have shown publicly their support of measures to prepare in case of bioterrorism events. The American Dental Association and local dental societies play an important role in disseminating information about the system in coordination with local, state, and federal public health agencies.

12.14 Conclusion

On March 2018, the Journal of the American Dental Association reported on an outbreak of bacterial endocarditis associated with infection control practices at an oral surgery practice (Ross et al. 2018). Their investigation occurred as a result of a clever infectious disease physician noticing the occurrence of two patients with no known risk factors being diagnosed with E. faecalis endocarditis.

Per the investigation conducted by the New Jersey Department of Health (NJDOH), in coordination with the NJ Board of Dentistry, further cases were identified. The NJDOH utilized their NJ Discharge Data Collection System (NJDDCS) to identify the other cases using ICD-9 billing diagnostic codes. This lead to the identification of 15 cases linked to the practice. Due to the time that had passed since the original cases occurred, there was no chance to use molecular sequencing or matching. As a result of the infection, 12 patients underwent surgery and one died. This is an example, where, in the future, biosurveillance systems could play a significant role in identifying real time or near real time increases of cases (or in an expanded geographical area) that compel further investigation. Again, biosurveillance systems could be of benefit, not only in extreme circumstances (like catastrophic man made public health events), but also as part of ongoing public health activities.

As mentioned by Dr. DePaola (National Institute of Dental and Craniofacial Research 2004) dentists may "have little to offer" in specific biosurveillance scenarios, yet the integration of different technologies can change this perception. Goldenberg et al. (2002) described over-the-counter medication sales as a technique for discovering disease outbreaks and stated that their approach may be "more timely" than traditional medical or public health approaches. Medical cases that result from bioterrorism attacks do not produce symptoms until they have fully developed, so it is likely that different patterns can be detected before the patients start reaching the Emergency Department. In the case of dentistry, Torres-Urquidy et al. (2009) established that using oral manifestations may allow for detecting a bioterrorism event up to 24 h prior to other signals using other forms of surveillance.

Public health events, at least at their inception, are intrinsically local events. Dr. Krolls (National Institute of Dental and Craniofacial Research 2004; Munson and Vujicic 2016) in his final remarks during his presentation at the Dentistry's Role Conference Against Bioterrorism, said, "dentists may pick up tell-tale information about what is happening in the community. After all, dentists spend more time with their patients than any other health specialty."

Disclaimer The views presented in this chapter are solely of the authors and do not necessarily represent the views of the US Government, Department of Health and Human Services and/or the Centers for Disease Control and Prevention.

References

Acharya A, Schroeder D, Schwei K, Chyou PH. Update on electronic dental record and clinical computing adoption among dental practices in the United States. Clin Med Res. 2017;15(3-4):59–74. https://doi.org/10.3121/cmr.2017.1380. Epub 11 Dec 2017

Bayer R, Colgrove J. Bioterrorism, public health and the law. Health Aff (Millwood). 2002;21(6):98–101.

Chapman WW, Bridewell W, Hanbury P, et al. Evaluation of negation phrases in narrative clinical reports. Proc AMIA Symp. 2001:105–9.

Chasteen JE, Murphy G, Forrey A, Heid D. The health insurance and portability and accountability act: practice of dentistry in the United States: privacy and confidentiality. J Contemp Dent Pract. 2003;1(4):59–70.

Delrose DC, Steinberg RW. The clinical significance of the digital patient record. J Am Dent Assoc. 2000;131(Suppl):57S–60S.

Dixon MG, Schafer IJ, Centers for Disease Control and Prevention (CDC). Ebola viral disease outbreak—West Africa, 2014. MMWR Morb Mortal Wkly Rep. 2014;63(25):548–51.

Etzioni A. Public health Law: a communitarian perspective. Health Aff. 2002;21(6):102–4.

Fauci AS, Morens DM. Zika virus in the Americas—yet another arbovirus threat. N Engl J Med. 2016;374:601–4.

Fineberg HV. Pandemic preparedness and response—lessons from the H1N1 influenza of 2009. N Engl J Med. 2014;370(14):1335–42. https://doi.org/10.1056/NEJMra1208802.

Frist B. Public health and national security: the critical role of increased federal support. Health Aff. 2002;21(6):117–30.

Gesteland PH, Gardner RM, Tsui FC, et al. Automated syndromic surveillance for the 2002 Winter Olympics. J Am Med Inform Assoc. 2003;10(6):547–54. Epub 4 Aug 2003

Goldenberg A, Shmueli G, Caruana RA, Fienberg SE. Early statistical detection of anthrax outbreaks by tracking over-the-counter medication sales. Proc Natl Acad Sci U S A. 2002;99(8):5237–40.

Griebel L, Prokosch HU, Köpcke F, et al. A scoping review of cloud computing in healthcare. BMC Med Inform Decis Mak. 2015;15:17. https://doi.org/10.1186/s12911-015-0145-7.

Groseclose SL, Buckeridge DL. Public health surveillance systems: recent advances in their use and evaluation. Annu Rev Public Health. 2017;38:57–79. https://doi.org/10.1146/annurev-publhealth-031816-044348.

Guay AH. Dentistry's response to bioterrorism: a report of a consensus workshop. J Am Dent Assoc. 2002;133:1181–7.

Heid DW, Chasteen J, Forrey AW. The electronic oral health record. J Contemp Dent Pract. 2002;1(3):043–54.

Ivanov O, Wagner MM, Chapman WW, Olszewski RT. Accuracy of three classifiers of acute gastrointestinal syndrome for syndromic surveillance. Proc AMIA Symp. 2002:345–9.

Kindig D, Stoddart G. What is population health? Am J Public Health. 2003;*93*(3):380–3.

Lumpkin JR. Air, water, places, and data—public health in the information age. J Public Health Manag Pract. 2001;7(6):22–30.

Munson B, Vujicic M. Number of practicing dentists per capita in the United States will grow steadily. Health Policy Institute. American Dental Association. 2016. http://www.ada.org/~/media/ADA/Science%20and%20Research/HPI/Files/HPIBrief_0616_1.pdf. Accessed 17 June 2018.

Narcisi JP. The American dental association's commitment to electronic data interchange. J Dent Educ. 1996;60(1):28–32.

National Institute of Dental and Craniofacial Research. Dentistry's role in responding to bioterrorism and other catastrophic events. 2004. https://web.archive.org/web/20180104212106/https://www.nidcr.nih.gov/careersandtraining/DentistryCatastrophicEvents.htm. Accessed 17 June 2018.

Palmer C. Dental leaders review roles in bioterrorism response. ADA NEWS. 2003. https://web.archive.org/web/20060219190632/http://www.ada.org/prof/resources/pubs/adanews/adanews-article.asp?articleid=390. Accessed 17 June 2018.

Reshetin VP, Regens JL. Simulation modeling of anthrax spore dispersion in a bioterrorism incident. Risk Anal. 2003;23(6):1135–45.

Rhodes PR. The computer-based oral health record. J Dent Educ. 1996;60(1):14–8.

Ross KM, Mehr JS, Greeley RD, et al. Outbreak of bacterial endocarditis associated with an oral surgery practice: New Jersey public health surveillance, 2013 to 2014. J Am Dent Assoc. 2018;149(3):191–201. https://doi.org/10.1016/j.adaj.2017.10.002. Epub 2 Feb 2018

Schleyer TK. Integrating dental office technology—the next frontier. Dent Abstr. 2003;48(3):112–3.

Schleyer T, Eisner J. The computer-based oral health record: an essential tool for cross-provider quality management. J Calif Dent Assoc. 1997;22(11):57–64.

Schleyer TK, Spallek H, Bartling WC, Corby P. The technologically well-equipped dental office. J Am Dent Assoc. 2003;134(1):30–41.

Schleyer TK, Thyvalikakath TP, Spallek H, et al. Clinical computing in general dentistry. J Am Med Inform Assoc. 2006;13(3):344–52.

Sfikas PM. HIPAA security regulations protecting patients' electronic health information. J Am Dent Assoc. 2003;134:640–3.

Szekely DG, Milam S, Khademi JA. Legal issues of the electronic dental record: security and confidentiality. J Dent Educ. 1996;60(1):19–23.

Torres-Urquidy MH, Wallstrom G, Schleyer TK. Detection of disease outbreaks by the use of oral manifestations. J Dent Res. 2009;88(1):89–94.

Toth D. The best practice management software for your office. Dental Products Report. Dec 21. 2015. http://www.dentalproductsreport.com/dental/article/best-practice-management-software-your-office. Accessed 17 June 2018.

Tsui FC, Espino JU, Dato VM, et al. Technical description of RODS: a real-time public health surveillance system. J Am Med Inform Assoc. 2003;10(5):399–408.

US Department of Health and Human Services. HHS acting secretary declares public health emergency to address national opioid crisis. 2017. https://www.hhs.gov/about/news/2017/10/26/hhs-acting-secretary-declares-public-health-emergency-address-national-opioid-crisis.html. Accessed 17 June 2018.

Wagner MM, Moore AW, Aryel RM. Handbook of biosurvellance. Burlington: Elsevier Academic Press; 2006.

Wong WK, Moore A, Cooper G, Wagner M. WSARE: what's strange about recent events? J Urban Health. 2003;80(2 Suppl 1):i66–75.