

1 **Framework for Evaluating Public Health Surveillance Systems**

2 **For Early Detection of Outbreaks**

3
4
5 This framework for evaluating public health surveillance systems for early
6 detection of outbreaks is a work-in-progress of many interested public health
7 practitioners across the Centers for Disease Control and Prevention and our
8 partners in federal, state, and local health agencies, academia, the business sector,
9 and the military. This effort has been guided by the additional input of an expert
10 working group convened by CDC.

11 12 **Proper MMWR format will be needed here to recognize contributors** 13 **on the Working Group and others who submitted comments**

14 **CDC Evaluation Working Group on** 15 **Syndromic Surveillance Systems**

16
17
18 **Claire Broome, M.D.**

19 CDC/ Office of the Director

20
21 **James W. Buehler, M.D.**

22 Center for Public Health Preparedness &
23 Research, Dept of Epidemiology
24 Rollins School of Public Health,
25 Emory University

26
27 **Louise Gresham, Ph.D., M.P.H.**

28 San Diego Health and Human Services, Public
29 Health Services

30
31 **Richard Hopkins, M.D., M.S.P.H.**

32 CDC/ Division of Public Health Surveillance
33 and Informatics
34 Epidemiology Program Office

35
36 **Ken Kleinman, Sc.D.**

37 Harvard Pilgrim Health Care

38
39 **Farzad Mostashari, M.D., M.S.P.H.**

40 NYC Dept of Health and Mental Hygiene

41
42 **J. Marc Overhage, M.D., Ph.D.**

43 Indiana University School of Medicine

44

45 **Julie Pavlin, M.D., M.P.H.**

46 Walter Reed Army Institute of Research
47 Division of Preventive Medicine

48

49 **Robert Rolfs, M.D., M.P.H.**

50 Utah Department of Health
51 CDC/National Center for Chronic Disease
52 Prevention and Health Promotion

53

54 **Henry Rolka, R.N., M.P.S., M.S.**

55 CDC/ Division of Public Health Surveillance
56 and Informatics
57 Epidemiology Program Office

58

59 **David Siegrist, M.S., M.A.**

60 Research Fellow
61 Potomac Institute for Policy Studies

62

63 **Dan Sosin, M.D., M.P.H.**

64 CDC/ Division of Public Health Surveillance
65 and Informatics
66 Epidemiology Program Office

67

68 **Van Tong, M.P.H.**

69 CDC/Public Health Prevention Specialist
70 Epidemiology Program Office

71

72
73
74
75
76
77
78
79
80
81
82
83
84
85
86

Corresponding author:

Daniel M. Sosin, M.D., M.P.H.
Director, Division of Public Health Surveillance and Informatics
Epidemiology Program Office
Centers for Disease Control and Prevention
Mail stop K-74
4771 Buford Highway, NE
Atlanta, GA 30341-3717

86 **Introduction**

87 Public health surveillance is the ongoing, systematic collection, analysis, interpretation, and
88 dissemination of data regarding a health-related event for use in public health action to reduce
89 morbidity and mortality and to improve health (1). Surveillance serves many public health
90 functions, such as supporting case detection and public health interventions, estimating the
91 impact of a disease or injury, portraying the natural history of a health condition, determining the
92 distribution and spread of illness, generating hypotheses and stimulating research, evaluating
93 prevention and control measures, and facilitating planning (2). One important public health
94 function of surveillance is outbreak detection -- identifying a rise in frequency of disease above
95 the background occurrence of the disease.

96 Outbreaks have typically been recognized either based on accumulated case reports of
97 reportable diseases, or by alert clinicians and laboratorians who bring clusters of diseases to
98 public health attention. Driven by the threat of bioterrorism and the increasing availability of
99 electronic health data, an array of new surveillance systems have been developed and
100 implemented in public health jurisdictions with the goal of early and complete detection of
101 outbreaks (3). In general, these new systems, loosely termed ‘syndromic surveillance,’ use data
102 that are not diagnostic of a disease but which might provide an indication of the early stages of
103 an outbreak. The utility of new systems for early detection and response to outbreaks has not
104 been well established and significant costs are incurred in developing and managing these
105 surveillance systems and investigating false alarms (4). Focused attention to the measurement of
106 the performance of public health surveillance systems for outbreak detection is needed to
107 establish the relative value of different approaches and to improve their efficacy for detection of
108 outbreaks at the earliest stages.

109 This report supplements existing CDC guidelines for evaluating public health surveillance
110 systems (1) by focusing on the measurement of timeliness for outbreak detection and the balance
111 among sensitivity, predictive value positive (PVP), and predictive value negative (PVN) for
112 detecting outbreaks. These guidelines encourage detailed description of system design and
113 operations and their experience with outbreak detection.

114 The framework is best applied to systems that have data available to demonstrate the
115 attributes of the system under consideration. Nonetheless, this framework can also be applied to
116 systems that are in early stages of development or in the planning phase. Attributes can be

117 addressed hypothetically and justified through the citation of published literature if actual data
118 are unavailable.¹ Ideally, the evaluation should compare the performance of the surveillance
119 system under scrutiny to alternative surveillance systems and produce an assessment of the
120 relative utility for early detection of outbreaks.

121

122 **Background**

123 Early outbreak detection can be achieved a) by assuring timely and complete receipt, review,
124 and follow-up of disease case reports (i.e., prompt reporting and consultation by physicians,
125 health care facilities, and laboratories consistent with disease reporting laws), b) by responding
126 to smaller signals indicating possible events of interest (i.e., lowering the threshold for
127 investigating possible outbreaks, or using modeling tools to improve the predictive value of data
128 at an earlier stage of the outbreak), and c) through receipt of new types of data that can signify an
129 event earlier in its course (5).

130 The foundation of infectious disease outbreak detection in the United States is the state and
131 local application of the reportable disease surveillance system known as the National Notifiable
132 Disease Surveillance System (NNDSS) (<http://www.cdc.gov/epo/dphsi/nndsshis.htm>). NNDSS
133 includes the explicit listing of diseases and laboratory findings of public health interest, the
134 publication of case definitions for their surveillance, and a system for passing case reports from
135 local to state to national public health agencies. This process occurs best in a context where
136 there is two-way communication between public health agencies and the clinical community:
137 clinicians and laboratories report cases and clusters of cases of reportable and unusual diseases,
138 while health departments provide consultation on case diagnosis and management, alerts,
139 surveillance summaries, and clinical and public health recommendations and policies. On-going
140 health care provider and laboratory outreach, education, and access to public health professionals
141 at all times are needed to enhance reporting. Electronic laboratory reporting (i.e., the automated
142 transfer of designated data from a laboratory database to a public health data repository using a
143 defined message structure) may also improve the timeliness and completeness of reporting
144 notifiable conditions (6,7,8) and can serve as a model for electronic reporting of a wider range of
145 clinical information. The comprehensive surveillance effort includes supporting timely

¹ An annotated bibliography on syndromic surveillance is available at
<http://www.cdc.gov/epo/dphsi/syndromic/index.htm>

146 investigation, tracking, and data needs for managing the public health response to an outbreak or
147 terrorist event. This document does not specifically address the evaluation of reportable disease
148 surveillance systems; however, the framework does address their value in early recognition of
149 outbreaks.

150

151 **Definition of Syndromic Surveillance**

152 Many new surveillance systems and methods for early detection have been labeled as
153 syndromic surveillance. The scope of this framework is broader than these innovative systems,
154 yet the wide-ranging definitions and expectations of syndromic surveillance invite clarification.
155 Syndromic surveillance for early outbreak detection is an investigational approach where health
156 department staff, assisted by automated data acquisition and generation of statistical alarms,
157 monitor disease indicators continually (real-time) or at least daily (near real-time) to detect
158 outbreaks of diseases earlier and more completely than would otherwise be possible with
159 traditional public health methods (e.g., by reportable disease surveillance, telephone
160 consultation, etc.). Automated analysis and visualization tools are applied to screen data for
161 unexpected patterns warranting further public health investigation. What most distinguishes
162 syndromic surveillance from other approaches, however, are the indicator data types (e.g., test
163 requests), which are distinct from the data sources (e.g., laboratories). A wide variety of data
164 types have been used by public health for syndromic surveillance, reflecting events that precede
165 clinical diagnosis, such as emergency department chief complaints, clinical impressions on
166 ambulance run sheets, prescriptions filled, retail drug and product purchases, school or work
167 absenteeism, and constellations of medical signs and symptoms in persons seen in various
168 clinical settings. Thus, syndromic surveillance systems emphasize timely and complete data
169 collection through electronic data sharing, the use of statistical tools to recognize outbreaks, and
170 the reporting of data about people with outbreak-related diseases early in their clinical course,
171 before a disease diagnosis has been assigned. Yet only the data type is unique to syndromic
172 surveillance.

173

174 **Purposes of Syndromic Surveillance**

175 Three related purposes for implementing syndromic surveillance have emerged:

- 176 • disease case detection and case management,

- 177 • outbreak management, and
- 178 • outbreak detection,

179 Syndromic surveillance has been used to screen for cases of disease when the condition is
180 infrequent and the syndrome is relatively specific for the condition of interest. Acute flaccid
181 paralysis is a syndromic marker of poliomyelitis and is used to detect single cases of suspected
182 polio in a timely way to initiate investigation and control measures. Here the syndrome is
183 relatively uncommon and serious, and serves as a proxy for polio (9). Syndromic surveillance
184 has also been used effectively in resource-poor settings for sexually-transmitted disease detection
185 and control where lab confirmation is not possible or practical (10). Syndromic surveillance for
186 terrorism, however, has limitations for early detection of single cases or small outbreaks because
187 early clinical manifestations of diseases that may be due to terrorism are common and
188 nonspecific (11). Individual case detection and follow-up investigation of all persons with non-
189 specific syndromes that could be due to one of the terrorism agents would put unreasonable
190 demands on public health staff and is not a viable goal.

191 Enhanced case-finding and monitoring the course and population characteristics of a
192 recognized outbreak have been proposed as benefits of syndromic surveillance (4) and a manual
193 system of syndromic surveillance was employed to detect anthrax cases in the fall of 2001 (12).
194 Severe Acute Respiratory Syndrome (SARS) is a disease defined by a syndrome. In epidemic
195 countries SARS could be tracked by clinical symptoms, whereas exposure history was needed in
196 countries where SARS was not epidemic. Since exposure history is not routinely available
197 through most existing electronic data resources, a short-term, intensive surveillance effort with
198 customized data collection for exposure history would be needed for enhanced case finding and
199 management during a known outbreak.

200 Outbreak detection is the overriding purpose for syndromic surveillance for terrorism
201 preparedness. This evaluation framework is oriented primarily to outbreak detection. Examples
202 of outbreak detection through syndromic surveillance include the onset of influenza season and
203 outbreaks of gastroenteritis (13-15). A related value of syndromic surveillance is reassurance
204 during a period of heightened risk of an outbreak. In order for reassurance to be credible, the
205 system must have a demonstrated ability to detect outbreaks of the kind and size being
206 dismissed. Additionally, the heightened interaction between public health departments and
207 clinical care providers in the conduct and follow-up of syndromic surveillance has also been

208 noted improve communication and the opportunity for reporting diseases of public health
209 interest.

210

211

212 **Framework**

213 This framework is intended to support the evaluation of all public health surveillance systems
214 for their timely detection of outbreaks. The framework is organized into four categories (system
215 description, outbreak detection, experience, and conclusions and recommendations) as shown in
216 the text box. A comprehensive evaluation will include information on all four categories.

Framework Outline

A. System Description

1. Purpose: what is the system designed to accomplish?
2. Stakeholders: who is the system serving?
3. Operation: how does the system work?

B. Outbreak Detection

1. Timeliness: how early in the disease process or outbreak is the event detected?
2. Validity: how well does the system perform in outbreak detection and distinguishing outbreaks of public health significance from unimportant events or random variations in disease trends?

C. Experience

1. System Usefulness: in what ways has the system demonstrated value relevant to public health?
2. Flexibility: how adaptable is the system to changing needs and risk thresholds?
3. System Acceptability: have stakeholders been willing to contribute to and use the system?
4. Portability: how readily can the system be duplicated in another location?
5. System Stability: how consistent has the system been in providing access to reproducible results?
6. System Costs: what are the resource requirements to deploy and maintain the system?

D. Conclusions and Recommendations for Use and Improvement of the Syndromic Surveillance System

217

218

219

220 **A. System Description**

221

222 A.1. Purpose

223 The purpose(s) of the system needs to be explicitly and clearly described. The
224 description of purpose should capture the intended uses of the system. The evaluation
225 methods might be prioritized differently for different purposes (e.g., reassurance requires
226 greater emphasis on the predictive value of negative results). The description of purpose
227 should include the indications for implementing the system, whether the system is designed
228 for short-term, high-risk situations or long-term, continuous use, the context in which the
229 system operates (whether it stands alone or augments data from other surveillance systems),
230 what type of outbreaks this system is intended to detect, and what secondary functional value
231 is desired. Designers of the system should state how sensitive or how specific they want the
232 system to be and whether it is intended to capture small or only large events.

233

234 A.2. Stakeholders

235 List the stakeholders of the system. Stakeholders include those who provide data for the
236 system as well as those who use the information generated by the system (e.g., public health
237 practitioners; health care practitioners; other health-related data providers; public safety
238 officials; government officials at local, state, and federal levels; community residents; non-
239 governmental organizations; commercial systems developers). The stakeholders might vary
240 among different systems and might change with time. Listing current stakeholders helps
241 define who the system is intended to serve, providing context for the evaluation results.

242

243 A.3. Operation

244 All aspects of the operation of the syndromic surveillance system should be described in
245 detail to allow stakeholders to validate the description of the system and for other interested
246 parties to understand the complexity and resources needed to operate such a system.

247 Detailed system description will also facilitate evaluation by highlighting variations in
248 system operation that are relevant to variations in system performance. Figure 1 depicts
249 stages of surveillance for early outbreak detection. Such a conceptual model can facilitate
250 the description of the system. The description of the surveillance process should address:

251

- System wide characteristics

- 252 • Data flow, see Figure 2
- 253 • Data and transmission standards to facilitate interoperability and data
- 254 sharing between information systems
- 255 • Security
- 256 • Privacy and confidentiality
- 257 • Data sources (used broadly in this framework to include the data producing
- 258 facility [i.e., the entity sharing data with the public health surveillance system],
- 259 the data type [e.g., chief complaint, discharge diagnosis, lab test order], and the
- 260 data format [e.g., electronic or paper, text descriptions of events or illnesses or
- 261 structured data reworded or stored in standardized format])
- 262 • Data processing before analysis (the data collation, filtering, transformation, and
- 263 routing functions required for public health to use the data; including the
- 264 classification and assigning of syndromes)
- 265 • Statistical analysis (tools for automated screening of data for potential outbreaks
- 266 [pattern recognition])
- 267 • Epidemiologic analysis, interpretation, and investigation (the rules, procedures,
- 268 and tools that support decision-making in response to a system alarm, including
- 269 adequate staffing with trained epidemiologists who can review, explore, and
- 270 interpret the data in a timely manner)

271

272 A detailed checklist is included in Appendix A.

273

274 **B. Outbreak Detection**

275 The ability of a system to detect an increase in incidence of disease above background (i.e.,
276 an outbreak) at the earliest possible stage depends on:

- 277 • the timely capture and processing of the data produced by transactions of health
- 278 behaviors (e.g., over-the-counter pharmaceutical sales, emergency department
- 279 visits, nurse call line volume) or health care activities (e.g., laboratory test
- 280 volume, triage categorization of chief complaint) that may indicate an outbreak
- 281 • the validity of the data collected for measuring the conditions of interest at the
- 282 earliest stage of illness and the quality of those data

- 283 • the detection methods applied to this processed surveillance data to distinguish
284 routine events from those indicative of an outbreak

285

286 **B.1. Timeliness**

287 The timeliness of all surveillance approaches for outbreak detection, including syndromic
288 surveillance, is measured by the lapse of time from exposure to the initiation of a public
289 health intervention. Although measuring all of the time points that define intervals may be
290 impractical or inexact in an applied outbreak setting, measuring intervals in a consistent way
291 can be used to compare alternative outbreak detection approaches and specific surveillance
292 systems with one another. Figure 3 depicts a timeline with milestones and intervals from
293 exposure to public health intervention.

- 294 0. Exposure: By anchoring the timeline on exposure, the timeliness advantage of
295 different data sources can be assessed and compared. Exposure can most easily
296 be estimated in a point source outbreak. Time of exposure is often inferred
297 from knowledge of the agent (e.g., incubation period) and the epidemiology of
298 the outbreak.
- 299 1. Symptom onset: The interval to symptom onset in each case is defined by the
300 incubation period for the agent. Time of symptom onset might be estimated
301 using case interviews or existing knowledge of the agent together with the
302 exposure onset. The incubation period may vary in individuals according to
303 host factors and the route and dose of the exposure.
- 304 2. Behavior: Following symptom onset, a range of possible health behaviors can
305 occur (e.g., purchase over-the-counter medication from a store, call in sick to
306 work, visit an urgent care center, etc). When an affected person interacts with
307 the health care system, a range of provider health care behaviors may be
308 performed (e.g., order of a laboratory test, admission to hospital). The
309 selection of data sources for a system has a strong influence on timeliness.
310 Some fraction of those experiencing symptoms will initiate a health or health
311 care behavior which is a necessary step to being captured in the surveillance
312 system.

- 313 3. Capture in a record: How soon a behavior of an affected individual is captured
314 by the data providing facility varies greatly by data type and can be influenced
315 by system design. A retail purchase may be entered in an electronic database at
316 the moment the transaction is completed or a record may not be generated in a
317 clinical setting for hours after health care was sought.
- 318 4. Data ready to share: Time is required for the facility providing the data to
319 process the data and produce the files needed for public health. Records might
320 be transmitted to a central repository only periodically (e.g., weekly). Data
321 form can influence processing time (e.g., transcription from paper to electronic
322 form, coding text-based data) as can data manipulations needed to de-identify
323 data and prepare necessary files.
- 324 5. Capture in public health surveillance system: The time required to transfer data
325 from the data providing facility to the public health entity varies according to
326 the frequency established for routine data transmission, but also by the data
327 transmission method (e.g., Internet, mail, courier).
- 328 6. Pattern recognition: Before analytic tools can be applied to the data in the
329 surveillance system, certain processing steps must be taken (e.g., categorization
330 into syndrome categories, application of case definition, data transformations).
- 331 7. Alerting: The detection algorithm's alerting interval is a product of how often
332 the algorithm is run and a report is generated and the capacity of the algorithm
333 to filter noise and detect an aberration as early in the course of the outbreak as
334 possible.
- 335 8. Investigation: The initiation of a public health investigation occurs when a
336 decision is made to acquire additional data. Analysis and judgment are applied
337 by public health professionals to the processed surveillance data and other
338 information on hand to decide whether new data collection is warranted to
339 confirm the existence of an outbreak. The challenge of interpreting data from
340 multiple surveillance systems could diminish potential advantages in
341 timeliness. The focus on outbreak detection allows for investigations of
342 potential outbreaks to proceed before a specific clinical diagnosis is obtained.

343 9. Intervention: When confirmation of an outbreak of public health significance
344 is confirmed, interventions can be implemented to control the severity of
345 disease and prevent further spread. Interventions may be of a general nature
346 directed to the recognition of an outbreak (e.g., apply respiratory infection
347 precautions and obtain clinical specimens for diagnosis) or can be specific to
348 the diagnosis as available (e.g., antibiotic prophylaxis, vaccination).

349

350 **B.2. Validity**

351 The validity of a given surveillance system for outbreak detection varies by multiple
352 outbreak scenarios and surveillance system factors. These factors can confound the
353 comparison of systems and must be carefully described in the evaluation. For example, the
354 minimum size of an outbreak that can be detected by a system cannot be objectively
355 compared unless the systems are identical or differences are accounted for in:

- 356 ■ Case definitions – which establish the specificity and sensitivity for the condition of
357 interest, based on the data source, data type, and response criteria.
- 358 ■ Baseline estimation – which determines the stability of the background occurrence of
359 cases and is affected by factors such as population size and geographic distribution.
360 The performance of detection algorithms will vary by the quality and duration and
361 inherent variability of baseline data.
- 362 ■ Reporting delays – which yield incomplete data, introducing bias that will diminish
363 the performance of detection algorithms.
- 364 ■ Data characteristics – including underlying patterns in the data (e.g., seasonal
365 variation) and systematic errors inherent in the data (e.g., product sales which
366 influence purchasing behaviors unrelated to illness)
- 367 ■ Outbreak characteristics – which result from agent, host, and environmental factors
368 that affect the epidemiology of the outbreak. For example, a large aerosol exposure
369 with an agent causing serious disease in a highly susceptible population will have
370 very different detection potential than an outbreak of similar size spread person-to-
371 person over a longer time and dispersed distribution.

- 372 ▪ Statistical analysis – which defines how data are screened for outbreak detection.
373 Detection algorithms have different performance characteristics under different
374 outbreak conditions.
- 375 ▪ Epidemiologic analysis, interpretation, and investigation – which are the procedures,
376 resources, and tools for analysis, interpretation, and response that can significantly
377 affect the ability to detect and respond to outbreaks.

378 Ideally, different approaches to outbreak detection can be evaluated under the same
379 conditions, thereby isolating the unique features of the system (e.g., data type) from the
380 outbreak characteristics and health department capacity.

381

382 The data needed to evaluate and compare the performance of surveillance systems for early
383 outbreak detection can be obtained from naturally-occurring outbreaks or through simulation.

384

385 **Naturally-occurring Outbreaks**

386 Controlled comparisons of surveillance systems will be due to the infrequency of
387 outbreaks, particularly due to agents relevant to bioterrorism, and the diversity of systems
388 and outbreak settings. Our understanding of the value of syndromic surveillance and other
389 surveillance approaches to early detection, however, will increase as we amass descriptions
390 of their experience with detecting and missing real outbreaks. Description of experience is
391 limited by not having a comparable means of measuring outbreak detection successes and
392 failures across systems and by the diversity of surveillance system and outbreak factors that
393 influence performance. The more that system and outbreak factors can be codified in a
394 standard way, the better our ability to compare experience across systems. Descriptive
395 evaluation should include as much detail as can be provided in order to improve our
396 understanding of how representative naturally-occurring outbreaks are of bioterrorism-related
397 outbreaks and until we have a shared vocabulary for critical data elements. Proxy outbreak
398 scenarios reflect the types of naturally-occurring outbreaks that should not be missed if we
399 are to have confidence in the ability of these systems to detect outbreaks due to bioterrorism.

400 Examples of proxy events or outbreaks may include:

401 *Seasonal events*

- 402 ▪ Seasonal increases in influenza (most years)

- 403 ▪ Seasonal increases in Norovirus gastroenteritis (winter vomiting disease, Norwalk
404 gastroenteritis)
- 405 ▪ Unusually large seasonal increases due to other infectious respiratory agents --
406 parainfluenza, adenovirus, etc.

407 *Community outbreaks*

- 408 ▪ Large foodborne outbreaks (large in relation to the size of the city or neighborhood in
409 which they occur)
- 410 ▪ Large waterborne outbreaks
- 411 ▪ Large hepatitis A outbreaks
- 412 ▪ Large day-care-associated shigellosis outbreaks
- 413 ▪ Large legionellosis outbreaks
- 414 ▪ Coccidiomycosis and histoplasmosis outbreaks in endemic locations

415

416 Ideally, the measurement of outbreaks detected and false alarms would be designed as a
417 routine part of the any system workflow and carried out with minimal effort or complexity.

418 Routine reporting should be automated where possible. Relevant information needs include:

- 419 ▪ the number of statistical aberrations detected at a set threshold in a defined period of
420 time (e.g. frequency per month at a given p-value);
- 421 ▪ the action taken as a result of the alarms (e.g., review for data errors, in-depth follow-up
422 analysis of the specific conditions within the syndrome category, manual
423 epidemiological analysis to characterize an alarm, examining data from other systems,
424 increasing the frequency of reporting from affected sites);
- 425 ▪ the resources directed to the follow-up of the alert;
- 426 ▪ the public health response that resulted (e.g., an alert to clinicians, a vaccination
427 campaign, no further response);
- 428 ▪ an assessment of the value of the follow-up effort (e.g., that the effort was an appropriate
429 application of public health resources); and
- 430 ▪ detailed description of the agent, host, and environmental conditions of the outbreak will
431 also be important for comparing performance experiences.

432

433 In order to evaluate the relative value of different methods for outbreak detection, a direct
434 comparison approach is needed. For example, if a health department detects a significant
435 number of its outbreaks through telephone consultations, then a phone call tracking system
436 might produce the data needed to compare telephone consults with other approaches for early
437 detection of outbreaks.

438

439 **Simulation**

440 As an alternative to naturally occurring outbreaks, simulations can allow for the control
441 and modification of these factors to study system performance across a range of common
442 scenarios. Simulations, however, are limited in their ability to mimic the diversity and
443 unpredictability of real-life events. When possible, simulated outbreaks should be
444 superimposed on historical trend data. To evaluate detection algorithms comparatively, a
445 widely-available challenge problem and data set would be helpful. Simulation is limited by
446 the availability of well-documented outbreak scenarios (e.g., organism or agent
447 characteristics, transmission characteristics, population characteristics – including health
448 behaviors, environmental characteristics). Simulations should incorporate data for each of
449 the factors described in the beginning of the Validity subsection (B.2). Multiple simulation
450 runs should be used to test algorithm performance in different outbreak scenarios, allowing
451 for generation of operating characteristic curves that reflect performance in a range of
452 conditions.

453

454 **Component Validation Studies**

455 Focused studies to validate the performance of limited aspects of systems (e.g., data
456 sources, case definitions, statistical methods, timeliness of reporting) can provide indirect
457 evidence of system performance. Component studies can also test assumptions about
458 outbreak scenarios and support better data simulation. Syndrome case definitions for some
459 specific data sources need to be validated. Component validation studies should emphasize
460 outbreak detection over case detection. These studies should be designed to answer cross-
461 system issues, contain explicit hypotheses and research questions, and be shared in a manner
462 to advance the development of outbreak detection systems without unnecessary duplication.

463

464 Statistical Assessment of Validity

465 Surveillance systems must balance the risk of an outbreak, the value of early intervention,
466 and the finite resources for investigation. Perceived high risk and high value of timely
467 detection support high sensitivity and low thresholds for investigation. A low threshold can
468 prompt resource intensive investigations and tie up vital staff, while having a high threshold
469 may delay detection and intervention. The perceived threat of an outbreak, the community
470 value attached to early detection, and the investigation resources may vary over time. Thus it
471 may be difficult to set a fixed relationship between optimal sensitivity and predictive value
472 for purposes of evaluation.

473 The sensitivity and predictive value positive (PVP) and negative (PVN) are closely linked
474 and considered together in this framework. Sensitivity is the percentage of outbreaks
475 occurring in the jurisdiction detected by the system. PVP reflects the probability of a system
476 alarm being an outbreak. PVN reflects the probability that no outbreak is occurring when the
477 system does not yield an alarm. The calculation of sensitivity and predictive value is
478 described in detail in the updated guidelines for evaluating public health surveillance systems
479 (1). Measurement of sensitivity requires an alternative data source of high quality (e.g.,
480 “gold” standard) to confirm outbreaks in the population that were missed by the syndromic
481 surveillance system. Sensitivity for outbreak detection could be assessed through capture-
482 recapture techniques with two independent data sources (16). The high costs involved with
483 responding to false alarms and with delayed response to outbreaks demand efforts to quantify
484 and limit the impact of both. While the likelihood of terrorism is extremely low, the PVP
485 will remain near zero and a certain level of non-terrorism alarms will be a necessary part of
486 conducting surveillance for the detection of terrorism. It is possible to achieve better
487 performance in one attribute (e.g., sensitivity) without a performance decrement in another
488 (e.g., PVP) by changing the system (e.g., adding a data type; applying a better detection
489 algorithm). Improving sensitivity by simply lowering the cut-off for signaling an outbreak
490 will reduce PVP. Sensitivity and PVP for these surveillance systems will ultimately be
491 calibrated in each system to balance the secondary benefits (e.g., detection of naturally-
492 occurring outbreaks, disease case finding and management, reassurance on no outbreak
493 during periods of heightened risk, stronger reporting and consultation relationships between
494 public health and clinical medicine) with the locally acceptable level of false alarms.

495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525

Data Quality

The validity of syndromic surveillance system data is dependent on data quality. Error-prone systems and data prone to inaccurate measurement can negatively affect detection of unusual trends. Although data quality may be a less critical issue for screening common, non-specific indicators for statistical aberrations, quality should be evaluated and improved to the extent possible. Measuring data quality is dependent on a “gold standard” (e.g., medical record review or fabricated test data with values known to the evaluator). The updated guidelines for evaluating public health surveillance systems (1) describe data quality in additional detail.

- **Representativeness:** When case ascertainment within a population is incomplete (e.g., in a sentinel system or a statistically based sample), representativeness reflects whether a system accurately describes the distribution of cases by time, place, and person. Geographic representativeness is particularly important for detecting outbreaks of infectious diseases.
- **Completeness of data:** The frequency of unknown or blank responses to data items in the system can be used to measure the level of completeness. For systems that update data from prior transmissions, time should be factored into measurement by indicating the percentage of records that are complete (i.e., all variables are captured for a record) upon initial report and within an appropriate interval (e.g., 48 hours) of submission. Sites with significant reporting delays can be flagged for reliability concerns and targeted for improvement. Incomplete data can require follow-up before analysis, with associated reduction in timeliness and increase in cost. When multiple data providers contribute to a common data store for statistical analysis, the percentage of reporting sources that submit their data on a routine interval (e.g., every 24 hours) conveys the completeness of the aggregate database for routine analysis. Evaluation of completeness should include a description of the problems experienced with manual data management (e.g., coding errors or loss of data) and the problems with automated data management (e.g., programming errors or inappropriate filtering of data).

C. System Experience

526 The performance attributes described in this section convey the experience that has accrued
527 in using the system.

528

529 **C.1. System Usefulness**

530 A surveillance system is useful for outbreak detection insofar as it contributes to the early
531 detection of outbreaks of public health significance and allows for a more effective
532 intervention as a result. An assessment of usefulness goes beyond detection to address the
533 impact or value added by its application. Measurement of usefulness is inexact. As with
534 validity (B.2.), measurement will benefit from common terminology and standard data
535 elements. In the interim, detailed efforts to describe and illustrate the consequences of early
536 detection efforts will improve our understanding of their usefulness.

537 Evaluation should begin with a review of the objectives of the system and should
538 consider the priorities. Although fundamentally interested in the early detection of
539 intentional outbreaks of disease (i.e., terrorism), usefulness can also be addressed through the
540 early detection of any outbreak of public health importance. To the extent possible,
541 usefulness should be described by the disease prevention and control actions taken as a result
542 of the analysis and interpretation of the data from the system.

543 The impact of the surveillance system should be contrasted with other mechanisms
544 available for outbreak detection. An assessment of usefulness should list the outbreaks
545 detected and the role that different methods played in the identification of each one. Provide
546 examples of how the system has been used to detect or track health problems other than
547 outbreaks in the community. Describe the public health response to the outbreaks and health
548 problems detected. Describe how data from new surveillance systems support inferences
549 about disease patterns that would not be possible without new systems.

550 Surveillance systems for early outbreak detection are sometimes justified for the
551 reassurance they provide when aberrant patterns are not apparent during a heightened risk
552 period or when the incidence of cases declines during an outbreak. When community
553 reassurance is claimed as a benefit of the syndromic surveillance system, reassurance should
554 be defined and the measurement quantified (e.g., number of phone calls from the public on a
555 health department hotline; successful press conferences; satisfaction of public health
556 decision-makers; or resources to institutionalize the syndromic surveillance system).

557 Describe who is reassured and of what they are reassured. Reassurance should also be
558 evaluated for validity by estimating the PVN (B.2.a.)

559

560 **C.2. Flexibility**

561 The flexibility of a syndromic surveillance system refers to the system's ability to change as
562 needs change. The adaptation to changing detection needs or operating conditions should occur
563 with minimal additional time, personnel, or other resources. Flexibility generally improves the
564 more data processing is handled centrally rather than distributed to individual data providing
565 facilities because fewer system and operator behavior changes are needed. Flexibility should
566 address the ability of the system to apply evolving data standards and code sets (e.g., HL-7; ICD-
567 9 to ICD-10; SNOMED) as reflected in PHIN (<http://www.cdc.gov/phin/>). Flexibility includes
568 the adaptability of the system to shift from outbreak detection to outbreak management. The
569 flexibility of the system to meet changing detection needs can include the ability to add unique
570 data to refine signal detection; to capture exposure and other data relevant to managing an
571 outbreak; to add data providers to increase population coverage and detect or track low
572 frequency events; to modify case definitions (the aggregation of codes into syndrome groupings),
573 to improve the detection algorithm to filter random variations in trends more efficiently, and to
574 adjust the detection threshold. System flexibility is needed to balance the risk of an outbreak, the
575 value of early intervention, and the resources for investigation as our understanding of these
576 factors changes.

577

578 **C.3. System Acceptability**

579 As with the routine evaluation of public health surveillance systems (1), the acceptability of a
580 surveillance system for early outbreak detection is reflected by the willingness of participants
581 and stakeholders to contribute to the data collection, analysis, and use. This concept includes the
582 authority and willingness to share electronic health data and should include an assessment of the
583 legal basis for the collection of pre-diagnosis data and the implications of privacy laws, such as
584 the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule (17). All states
585 have broad disease reporting laws that require reporting of diseases of public health importance
586 and many of these appear compatible with the authority to receive syndromic surveillance data
587 (18). The authority to require reporting of indicator data for individuals who lack evidence of a

588 reportable condition and in the absence of an emergency is less clear and needs to be verified by
589 jurisdictions. Acceptability may vary over time as the threat level, perceived value of syndromic
590 surveillance, and resources fluctuate.

591 Acceptability of a system may be inferred from the extent of its adoption. Acceptability is
592 reflected by the participation rate of potential reporting sources, by the completeness of data
593 reporting, and by the timeliness of person-dependent steps in the system (e.g., manual data entry
594 from emergency department logs as distinguished from electronic data from the normal clinical
595 workflow).

596

597 **C.4. Portability**

598 The portability of a surveillance system addresses how well the system could be duplicated in
599 another setting. Adherence to the Public Health Information Network standards
600 (<http://www.cdc.gov/phn/>) can enhance portability by reducing variability in the application of
601 information technology between sites. Reliance on person-dependent steps, including judgment
602 and action criteria (e.g., for analysis and interpretation) should be fully documented to improve
603 system portability. Portability is also influenced by the simplicity of the system. Provide
604 examples of the deployment of similar systems in other settings and describe the experience of
605 those efforts. Where examples are lacking, describe features of the system likely to support or
606 detract from portability.

607

608 **C.5. System Stability**

609 The stability of a surveillance system refers to how resilient it is to system changes (e.g.,
610 change in coding from ICD-9 to ICD-10). Stability can be demonstrated by the duration and
611 consistent operation of the system. System stability is distinguished from the reliability of data
612 elements within the system (i.e., the consistent representation of the condition under
613 surveillance), which is an aspect of data quality. Stability can be measured by the frequency of
614 system outages or downtime for servicing during periods of need, including downtime of data
615 providers, the frequency of personnel deficiencies from staff turnover, and budget constraints.
616 Ongoing support by system designers and evolving software updates may improve system
617 stability. Stability can also be reflected in the extent of control over costs and system changes
618 that the sponsoring agency maintains.

619

620 **C.6. System Costs**

621 Cost is a vital factor in assessing the relative value of syndromic surveillance for terrorism
622 preparedness. Cost-effectiveness analyses and data modeling are needed under a range of
623 scenarios to estimate the value of syndromic surveillance for outbreak detection and terrorism
624 preparedness (19). Improved methods of measuring cost and impact are needed as well. Costs
625 should be documented from the perspective of the health department. Costs borne by data
626 providers should be noted as well.

627 Direct costs include the fees paid for software and data, the personnel salary and support
628 expenses (e.g., training, equipment support, and travel), and other resources needed to operate
629 the system and produce information for public health decisions (e.g. office supplies, Internet and
630 telephone lines, and other communication equipment). Fixed costs for running the system
631 should be differentiated from the variable costs of responding to system alarms. Variable costs
632 include the cost of follow-up activities (e.g., for diagnosis, case-management, or community
633 interventions). Specifically, the cost of responding to false alarms represents a variable but
634 inherent inefficiency of syndromic surveillance that should be accounted for in the evaluation.
635 Similarly, the financial and public health costs of missing outbreaks entirely or recognizing them
636 late are variable costs. The cost savings of early detection must be substantiated. Costs vary
637 because the sensitivity and timeliness of the detection methods can be modified according to
638 changes in tolerance for missing outbreaks and for responding to false alarms. Similarly, the
639 threshold and methods for investigating system alarms can vary with the perceived risk and need
640 to respond. Costs from public health response to false alarms with traditional surveillance
641 systems need to be measured in a comparable way when assessing the relative value of
642 syndromic surveillance. Questions to answer include:

- 643 ▪ How many investigations were initiated as a result of these data?
- 644 ▪ What response and cost was incurred through follow-up of flagged events?
- 645 ▪ What were the indications for responding?
- 646 ▪ How much staff time was required for follow-up?
- 647 ▪ Was anxiety raised unnecessarily by false alarms?
- 648 ▪ Was benefit obtained (e.g., through improved communication and confidence in the
649 responsibility and performance of public health) when false alarms were investigated?

- 650 ▪ Who was affected?
- 651 ▪ What costs did partners incur in follow-up of alarms (e.g., medical record staff work,
652 clinical staff efforts, etc.)? Follow-up costs for false alarms should be distinguished from
653 costs related to investigations that uncover real outbreaks that warrant a public health
654 response.
- 655 ▪ Did the health department fail to respond to a true event because of complacency or the
656 response burden resulting from responding to false alarms?
- 657 ▪ Did late recognition of an outbreak result in unnecessary morbidity?
- 658 ▪ Have lessons learned from earlier events reduced costs as the system continues to
659 operate?

660

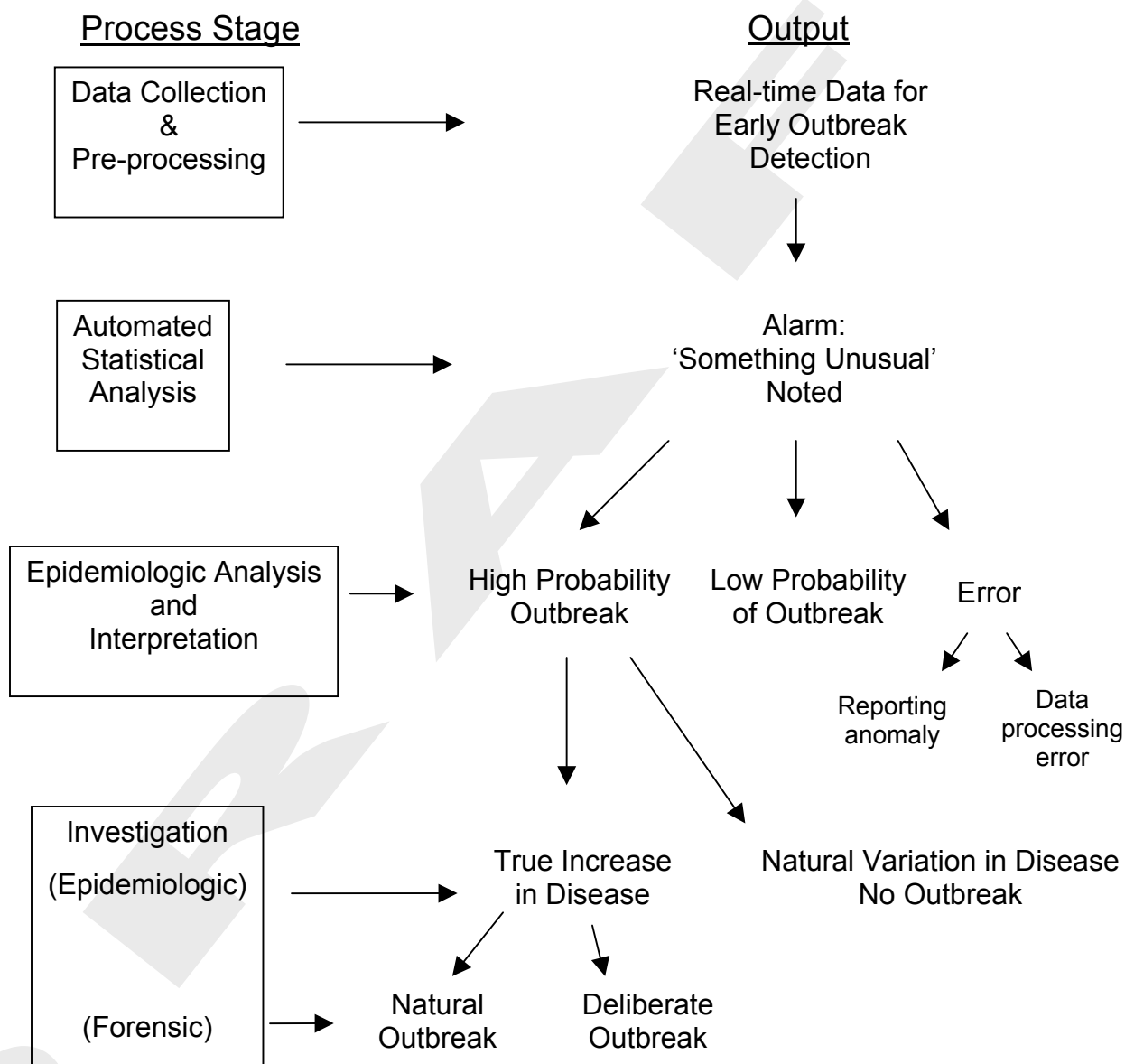
661 **D. Conclusions and Recommendations for Use and Improvement of Systems for** 662 **Early Outbreak Detection**

663 The evaluation should be summarized to convey the strengths and weaknesses of the system
664 under scrutiny. Summarizing and reporting evaluation findings should facilitate the comparison
665 of systems for those making decisions about new or existing surveillance methods. These
666 conclusions should be validated among stakeholders of the system and modified accordingly.
667 Recommendations should address adoption, continuation, or modification of the surveillance
668 system so that it can better achieve its intended purposes. Recommendations should be
669 disseminated widely and actively interpreted for all appropriate audiences.

670 As stated in a recent Institute of Medicine study on Microbial Threats to Health (19),
671 “[S]yndromic surveillance is likely to be increasingly helpful in the detection and monitoring of
672 epidemics, as well as the evaluation of health care utilization for infectious diseases” yet “a
673 balance should be sought between strengthening what is known to be helpful (e.g., diagnosis of
674 patients with infectious illness, strengthening of the liaison between clinical care providers and
675 health departments) and the exploration and evaluation of new approaches.” Guidance for the
676 evaluation of surveillance systems for outbreak detection is a work-in-progress. Many advances
677 are needed in our understanding of systems and outbreak characteristics to improve performance
678 metrics. For example, research is needed to understand the personal health and clinical health
679 care behaviors that might serve as early indicators of priority diseases; analytic methods are
680 needed to improve pattern recognition and to integrate multiple streams of data; a shared

681 vocabulary is needed for describing outbreak conditions, managing text-based information, and
682 supporting case definitions; and evaluation research is needed, including cost-effectiveness, of
683 different surveillance models for early detection, both in real-life comparisons and in simulated
684 data environments to characterize the size and nature of epidemics that can be detected through
685 innovative surveillance approaches. Despite the daunting needs, much can be learned today by
686 careful description of systems as directed by this framework.

Figure 1. Surveillance System Process Model for Early Outbreak Detection



687
688
689
690
691
692

692

693 Figure 2. Prototypical Surveillance Data Flow Chart for
694 Emergency Department Encounters

695
696

697
698

699
700

701
702

703
704

705
706

707
708

709
710

711
712

713
714

715
716

717
718

719
720

721
722

723
724

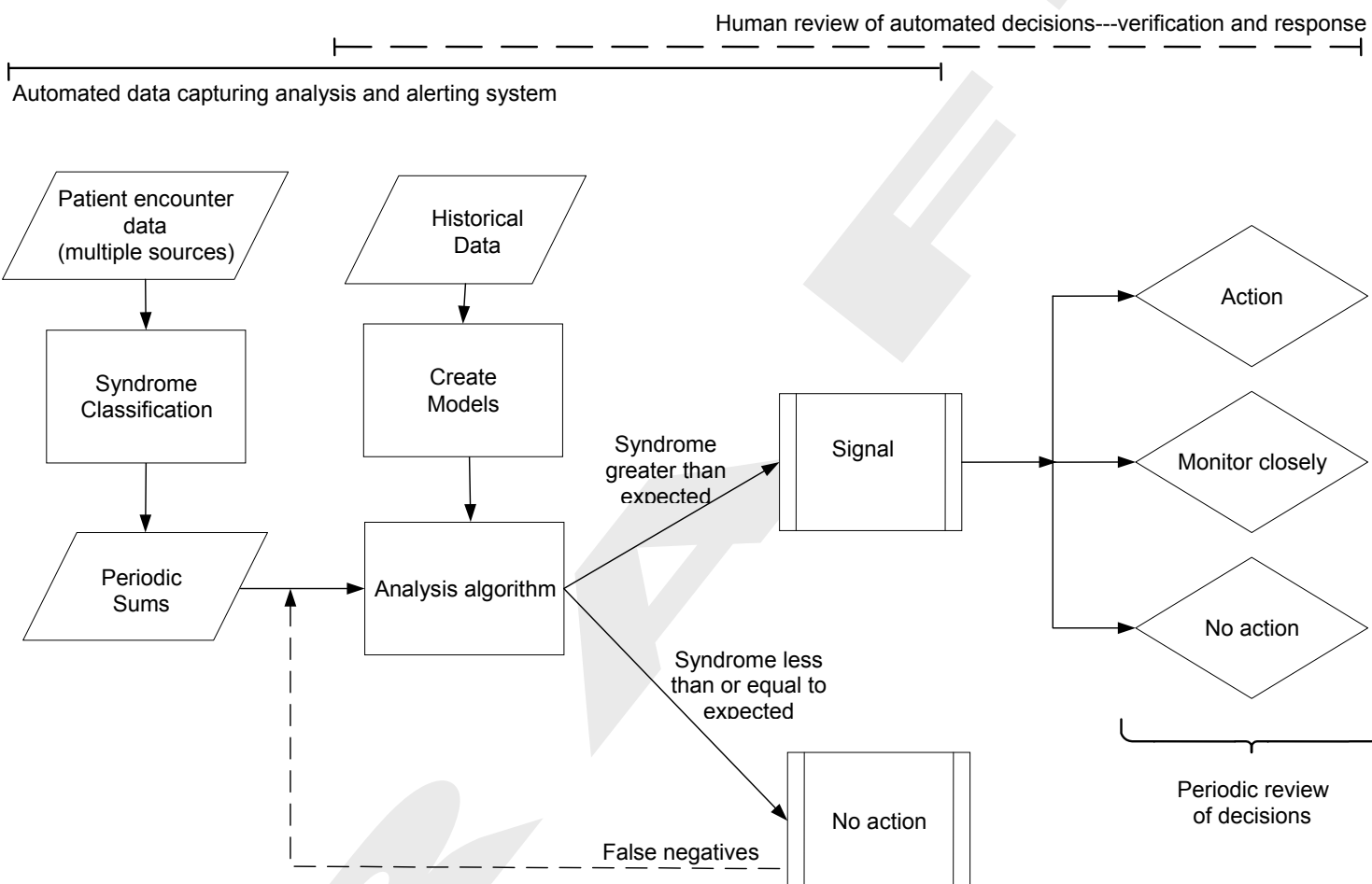
725
726

727
728

729
730

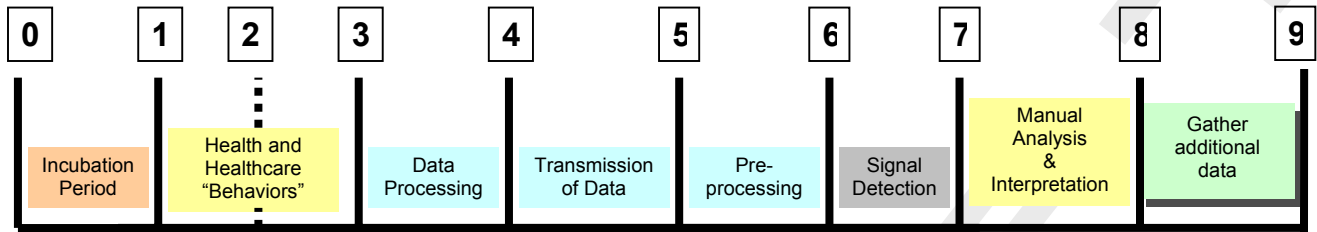
731
732

733
734



1. Patient records are captured in specified format (such as HL-7) and routed automatically to a computer.
2. Chief complaints from the HL-7 messages are used to classify the encounter into one of a number of syndrome categories.
3. Data are analyzed by a program that compares periodic sums with models developed from historical data.
4. Computer algorithm issues a signal when periodic sum statistically exceeds expected values (or a “no signal” if it does not).
5. Periodic review of “no alerts” is conducted to ensure correct decisions are being made.
6. Each alert is validated by an experienced epidemiologist, who makes a decision to initiate an investigation, closely monitor the situation or issue “no alert”
7. A periodic review of alert decision is also conducted for quality assurance.

Figure 3. Timeline Milestones



- 0. Point source exposure in time
- 1. Symptom onset
- 2. Behavior
- 3. Capture behavior in record
- 4. Data source ready to share
- 5. Capture data in surveillance system
- 6. Apply pattern recognition tools/ algorithms
- 7. Automated alert generation
- 8. Initiate public health investigation
- 9. Initiate public health intervention

735

736 **References**

- 737 1. Centers for Control and Prevention. Updated guidelines for evaluating public health
738 surveillance systems: recommendations from the guidelines working group. *MMWR*
739 2001;50(No. RR-13).
- 740 2. Teutsch SM, Churchill RE. *Principles and Practice of Public Health Surveillance*. 2nd
741 ed. Oxford University Press, Oxford; New York; 2000.
- 742 3. Lober WB, Karras BT, Wagner MM, Overhage JM, Davidson AJ, Fraser H, Trigg LJ,
743 Mandl KD, Espino JU, Tsui FC. Roundtable on bioterrorism detection: information
744 system-based surveillance. *J Am Med Inform Assoc* 2002;9(2):105-115.
- 745 4. Reingold A. If syndromic surveillance is the answer, what is the question? *Biosecurity*
746 *and Bioterrorism: Biodefense Strategy, Practice, and Science* 2003;1(2):1-5.
- 747 5. Wagner MM, Tsui FC, Espino JU, Dato VM, Sittig DF, Caruana RA, McGinnis LF,
748 Deerfield DW, Druzdzel MJ, Fridsma DB. The emerging science of very early detection
749 of disease outbreaks. *J Pub Health Mgmt Pract* 2001;(6):51-59.
- 750 6. Effler P, Ching-Lee M, Bogard A, Jeong MC, Nekomoto T, Jernigan D. Statewide system
751 of electronic notifiable disease reporting from clinical laboratories: comparing automated
752 reporting with conventional methods. *JAMA* 1999;282:1845-50.
- 753 7. Panackal AA, M'ikanatha NM, Tsui FC, McMahon J, Wagner MM, Dixon BW, et al.
754 Automatic Electronic Laboratory-based Reporting of Notifiable Infectious Diseases at a
755 Large Health System. *Emerg Infect Dis* [serial online] 2002 Jul;8;685-691. Available
756 from: URL: <http://www.cdc.gov/ncidod/EID/vol8no7/01-0493.htm#bac>
- 757 8. Hoffman MA, Wilkinson TH, Bush A, Myers W, Griffin RG, Hoff GL, et al.
758 Multijurisdictional approach to biosurveillance, Kansas City. *Emerg Infect Dis* [serial
759 online] 2003 Oct [date cited]. Available from: URL:
760 <http://www.cdc.gov/ncidod/EID/vol9no10/03-0060.htm>
- 761 9. Robertson SE, Suleiman AJM, Mehta FR, Al-Dhahry SHS, El-Bualy MS. Poliomyelitis
762 in Oman: acute flaccid paralysis surveillance leading to early detection and rapid
763 response to a type 3 outbreak. *Bull WHO* 1994;72(6):907-914.
- 764 10. Grosskurth H, Mosha F, Todd J, Mwijarubi E, Klokke A, Senkoro K, et al. Impact of
765 improved treatment of sexually transmitted diseases on HIV infection in rural Tanzania:
766 randomized controlled trial. *Lancet* 1995;346:530-6.

- 767 11. Zeng X, Wagner M. Modeling the effects of epidemics on routinely collected data. *Proc*
768 *AMIA Annu Symp* 2001:781-5.
- 769 12. Tan CG, Sandhu HS, Crawford DC, Redd SC, Beach MJ, Buehler JW, et al. Surveillance
770 for anthrax cases associated with contaminated letters, New Jersey, Delaware, and
771 Pennsylvania, 2001. *Emerg Infect Dis* [serial online] 2002 Oct [*October 1, 2003*];8.
772 Available from: URL: <http://www.cdc.gov/ncidod/EID/vol8no10/02-0322.htm>
- 773 13. Carrat F, Flahault A, Boussard E, Farran N, Dangoumau L, Valleron AJ. Surveillance of
774 influenza-like illness in France. The example of the 1995/1996 epidemic. *J Epidemiol*
775 *Community Health* 1998;52(Suppl 1):32S-38S.
- 776 14. Mostashari F, Fine A, Das D, Adams J, Layton M. Use of ambulance dispatch data as an
777 early warning system for communitywide influenzalike illness. *J Urban Health*
778 2003;80(2, suppl 1):i43-i49.
- 779 15. Pavlin JA. Investigation of disease outbreaks detected by “syndromic” surveillance
780 systems. *J Urban Health* 2003;80(2, suppl 1):i107-i114.
- 781 16. Yvonne M.M. Bishop, Stephen E. Fienberg, and Paul W. Holland. Discrete Multivariate
782 Analysis: Theory and Practice. Chapter 6: *Estimating the size of a closed population*.
783 MIT Press, 1975, pp. 229-256.
- 784 17. Centers for Disease Control and Prevention. HIPAA Privacy Rule and Public Health.
785 Guidance from CDC and the Department of Health and Human Services. *MMWR*
786 Supplement 2003;52(S-1):1-12.
- 787 18. Broome CV, Horton HH, Tress D, Lucido SJ, Koo D. Statutory Basis for Public Health
788 Reporting Beyond Specific Diseases. *J Urban Health* 2003;80(2, suppl 1):i14-i22.
- 789 19. Smolinski MS, Hamburg MA, Lederberg J. *Microbial Threats to Health: Emergence,*
790 *Detection, and Response*. Washington, DC: National Academies Press; 2003.
791

791 Appendix A. Operations Checklist

792

793 A. System-wide Issues

- 794 Describe the political, administrative, and geographic context for the system
- 795 Provide a process model that describes the data flow of the system:
 - 796 Who inputs the data into the system
 - 797 Who can view the data
 - 798 Who can manipulate the data
 - 799 Indicate where processing occurs centrally and where at distributed sites
 - 800 Indicate where steps are automated and where manual
 - 801 Indicate which steps are managed on-site and which can be done remotely
 - 802 Estimate the time required for each step of the data flow
 - 803 Indicate whether source data are produced in the course of routine workflow or
 - 804 specifically for the purpose of syndromic surveillance
- 805 Describe data and messaging standards:
 - 806 Identify standards used to facilitate interoperability
 - 807 Identify standards used to facilitate data sharing
 - 808 Describe how the system interfaces with other surveillance systems from the
 - 809 same sites to limit reporting burden
 - 810 Cite relevant PHIN standards and ability to meet them
 - 811 (<http://www.cdc.gov/phin/>)
 - 812 Provide legal documentation allowing data sharing
- 813 Describe procedures to maintain security:
 - 814 Indicate security procedures employed for transmission of data between sites
 - 815 and for data management at the central repository
 - 816 Describe security measures to protect data integrity at the central repository
 - 817 Cite relevant PHIN standards and ability to meet them
 - 818 (<http://www.cdc.gov/phin/>)
- 819 Describe procedures to assure privacy and confidentiality:
 - 820 Identify the legal authority under which the surveillance activity is being
 - 821 conducted
 - 822 Indicate the rules, procedures, and tools used to assure privacy and
 - 823 confidentiality, including methods for de-identification and re-identification, if
 - 824 used, and the points in the data flow where statistical disclosure limitation
 - 825 methods are applied

826 B. Data Sources

- 827 Describe the following:
 - 828 Data producing facility
 - 829 Data type
 - 830 Data format
 - 831 Data element definitions
 - 832 Code sets (e.g., International Classification of Diseases (ICD) codes) used to
 - 833 describe the response categories
 - 834 Data captured for geographic location (e.g., zipcode, geocode)
- 835 Provide a data model describing the relationship between data elements and the code sets
- 836 (The architecture of the National Electronic Disease Surveillance System (NEDSS

837 <http://www.cdc.gov/nedss/>) and the Public Health Conceptual Data Model
838 (<http://www.cdc.gov/nedss/DataModels/phcdm.pdf>) can serve as illustrations of
839 comprehensive data models.)

- 840 Indicate which data standards are used and whether they are proprietary
- 841 Identify the standards used for assembling data documentation (i.e., metadata)

842

843 C. Data Preprocessing

- 844 Indicate the steps taken to share data between information systems and indicate the
845 responsible organization for assuring each step (e.g., clinical facility, data clearinghouse,
846 local health department, state health department)
- 847 Indicate the frequency of data collection
- 848 Indicate the volume of data (e.g., average number of records per day)
- 849 Indicate how the accumulation of data is handled
- 850 Describe how different data streams or data elements are assembled, subset, and
851 manipulated to prepare them for analysis
- 852 Indicate whether a relational database is formed to link datasets and the unique
853 identifier(s) used for linkage
- 854 Indicate the health-related events, syndromes, or constellation of findings under
855 surveillance, including the derivation of the case-definitions
- 856 Identify who has authority to determine the criteria for case definitions and how case
857 criteria are applied to the data
- 858 Provide a description of any algorithms used to establish the status of a potential case
- 859 Indicate the frequency of editing and updating the electronic file
- 860 Indicate how incomplete records are handled in analysis and reports
- 861 Describe how data archiving and disposal is managed
- 862 Describe how new data sources or necessary changes in data sources are identified and
863 incorporated in the system.

864

865 D. Statistical Analysis

- 866 Describe how the health outcome baseline is established:
 - 867 Describe the population under surveillance
 - 868 Describe the source, the criteria, and the methods for establishing the background
869 frequencies used to detect aberrations
 - 870 How much baseline data are managed in the analysis database
- 871 Describe analytic methods used in automated analyses (i.e., aberration detection):
 - 872 Describe in mathematical and statistical detail the algorithms intended to signal an
873 event requiring further investigation
 - 874 Describe adaptations in analytic methods to account for different outbreak
875 patterns that might be anticipated in different data sources and types and for
876 different outbreak scenarios
 - 877 Indicate how reporting delays are corrected for in the analysis.
 - 878 Describe the method of adjusting results for potential confounding factors
 - 879 Describe how the system adapts over time and the empirical basis for
880 modifications in the methods
- 881 Describe the detection process:
 - 882 The frequency of data analysis

- 883 □ How an alarm is generated
- 884 □ Where the alarm goes
- 885 □ The type of alarms generated by the system
- 886 □ What is done to ensure that signals are not being missed
- 887 □ Describe the report generation process:
- 888 □ What routine reports are generated
- 889 □ Whether data are presented graphically or in tables
- 890 □ Whether data can be manipulated to get a specific table/chart
- 891 □ How often charts and tables are refreshed with new data
- 892 □ Indicate training level of personnel needed to manage the detection methods.
- 893

894 E. Epidemiologic Analysis, Interpretation, and Investigation

- 895 □ Describe the process for managing system alarms:
- 896 □ Describe the special procedures instituted when the alarm is generated (e.g.,
- 897 review for data errors, in-depth manual analysis of the specific conditions within
- 898 the syndrome category, manual epidemiological analysis to identify subgroups
- 899 responsible for an alarm, examining data from other systems, increasing the
- 900 frequency of reporting from affected sites)
- 901 □ Estimate the person-hours that are devoted to review and analysis each day and
- 902 the interval at which data are analyzed
- 903 □ Indicate documented procedures for managing system alarms.
- 904 □ Indicate communication method that staff is alerted of alarms (e.g., whether they
- 905 get paged at home, receive an automated e-mail, etc.?)
- 906 □ Indicate the expectations and schedule of staff to actively check the system and
- 907 schedule, including nights and weekends
- 908 □ Indicate the response options to an alarm and the factors that influence the choice
- 909 (e.g., wait for an alarm in another system, initiate an onsite investigation, alert
- 910 clinicians to gather information)
- 911 □ Describe the process for identifying cases for investigation when the data analyzed
- 912 routinely are unidentified
- 913 □ Describe how independent data types are integrated in the analysis for improved decision
- 914 making
- 915 □ Describe the rules, procedures, and tools for communication
- 916 □ Indicate the mechanisms used and content guidance provided for sharing results
- 917 with 1) reporting sources, 2) response community, and 3) the public;
- 918 □ Describe how decisions are made for sending urgent communications and the
- 919 methods for sending urgent communications
- 920 □ Indicate whether receipt of a communication is acknowledged and how
- 921 unacknowledged receipt is managed
- 922 □ Indicate how often urgent communications and routine reports are sent
- 923 □ Describe the protocol for conducting surveillance during outbreak management, if one
- 924 exists
- 925 □ Indicate how often data will be updated and analyzed
- 926 □ Describe how the system can be modified or customized to meet special data
- 927 needs

- 928 □ Describe how the system will monitor the impact of prevention and control
- 929 measures
- 930 □ Describe how and how often system components are tested for operational readiness
- 931 (e.g., ‘spiked’ data or modeling exercises)
- 932

933

933 **Appendix B. Tasks for Evaluating a Public Health Surveillance System for Early Detection**
934 **of Outbreaks**

935

936 **Task A. Describe the System**

- 937 1. Purpose: what is the system designed to accomplish?
938 2. Stakeholders: who is the system serving?
939 3. Operation: how does the system work?
940 a. System-wide Processes
941 b. Data Sources
942 c. Data Preprocessing
943 d. Statistical Analysis
944 e. Epidemiologic Analysis, Interpretation, and Investigation

945

946 **Task B. Provide Data Demonstrating Outbreak Detection Attributes**

- 947 1. Timeliness: how early in the outbreak is the event detected?
948 2. Validity: how well does the system perform in distinguishing outbreak detection of public health
949 significance from unimportant events or random variations in disease trends?
950 a. Sensitivity, specificity, & predictive value: what proportion of true cases and outbreaks are
951 detected by the system? What proportion of non-cases is detected as such? What proportion of alarms
952 triggered by the system are desired alarms (true positives)? What proportion of negative results is truly
953 negative?
954 b. Data quality: How does data quality affect validity of outbreak detection?
955 I. Representativeness: how well does the system reflect the population of interest?
956 II. Completeness: what percentage of data is present for each record?

957

958 **Task C. Describe the System Experience**

- 959 1. System Usefulness: in what ways has the system demonstrated value relevant to public health?
960 2. Flexibility: how adaptable is the system to changing needs and risk thresholds?
961 3. System Acceptability: have stakeholders been willing to contribute to and use the system?
962 4. Portability: how readily can the system be duplicated in another location?
963 5. System Stability: how consistent has the system been in providing access to reproducible results?
964 6. System Costs: what are the resource requirements to deploy and maintain the system?

965

966 **Task D. Conclusions and Recommendations for Use and Improvement of Systems for Early**
967 **Outbreak Detection**