Revisiones

Puntos de Gestión de Datos para Enfermedades Emergentes y Nuevas Herramientas de Vigilancia y Datos de Laboratorio

Stanley M. Martin, M.S., Nancy H. Bean, Ph.D.
Centers for Disease Control and Prevention, Atlanta, Georgia, USA Data Management Issues for Emerging Diseases

Desde 1976, cuando la enfermedad de los Legionarios afectó a los concurrentes a la Convención Estadounidense de Legionarios en Filadelfia (1), la extensión en salud pública se ha expandido. Durante la investigación del brote de 1976, la atención pública se centró en las noticias del número creciente de casos y muertes así como también a las especulaciones sobre las causas de las enfermedades y su prevención. Después del brote, los funcionarios de salud públicos lidiaron con grandes volúmenes de información, incluyendo datos clínicos, resultados de encuestas epidemiológicas, y registros de muestras recolectadas de pacientes y del ambiente. Esta información fue manejada en computadoras centrales.

En 1980, un grupo de casos de una enfermedad no reconocida, primariamente afectando a mujeres jóvenes, creó una situación de gestión de datos parecido a la que circundó al brote de la enfermedad de los Legionarios. Una investigación epidemiológica mayor, que incluyó el examen de una multitud de especímenes de laboratorio y volúmenes de datos analizados, fue emprendida por un gran equipo de funcionarios de salud pública federales, estatales, y locales, así como también de numerosas instituciones académicas e industrias privadas. Los problemas del establecimiento de bases de datos y la implementación de un sistema de gestión de datos para el síndrome de shock tóxico (2) fueron esencialmente los mismos que los problemas de gestión de datos de la enfermedad de los Legionarios, excepto que la tecnología de las computadoras se había adelantado ligeramente en las oficinas salud pública.

Durante la primavera de 1993, un grupo de casos de otra enfermedad desconocida, eventualmente atribuida a hantavirus (3), ocurrió en el sudoeste de los Estados Unidos. La reacción a esta enfermedad desconocida por los funcionarios de salud públicos reflejaron un hecho sorprendente: si bien los métodos de laboratorio y epidemiológicos para disminuir el brote estaban en su lugar, una estrategia de gestión de datos uniforme no se había establecido. Las bases de datos múltiples propósitos construidas *ad hoc* por los investigadores del brote comenzaron a empantanarse en la investigación. Los casos se registraron en bases de datos múltiples que no reconocieron informes de casos duplicados. Las actualizaciones de los datos de los casos se hicieron en algunos, pero no todas las bases de datos. Los datos de laboratorio sobre muestras de pacientes no fueron vinculados a otros datos clínicos y epidemiológicos sobre un paciente. Ninguna base de datos estuvo disponible con datos bien-editados, y completos acerca de todos los casos. Paralelamente, los esfuerzos fragmentados de manejo de datos involucrados en por lo menos 15 lugares, no fueron coordinados por ningún mecanismo para integrarlo en un sistema.

Introducir un solo sistema para la gestión de datos en el medio del brote de hantavirus involucró más de los puntos de gestión de datos sumados en los brotes iniciales. Previamente, la tecnología de la computadora fue considerada como una solución que, aunque algo engorrosa, permitió a los funcionarios moverse desde la gestión de datos manual a la gestión electrónica. Sin embargo, durante el brote de hantavirus, la tecnología de la computadora llegó a ser parte del problema; lo inicialmente previsto como una buena gestión de datos, pudo haber frustrado algunos de los esfuerzos de laboratorios y epidemiológicos para controlar el brote. Los datos esencialmente fueron cerrados en bases de datos diversas y no podrían ser analizados adecuadamente o combinados con datos en otras bases de datos. En algunos casos, esta circunstancia peculiar causó que los investigadores debieron realizar análisis manuales usando copias impresas de las bases de datos electrónicas o entrando los datos nuevamente en otros sistemas.

En años recientes, las consideraciones legales, tales como el Acto de Privacidad estatuido en 1974 y la Libertad de el Acto de Información estatuido en 1966 (4,5), también tienen complicados datos gestión. Estos actos, en sus esfuerzos para proteger la privacidad individual y asegurar la disponibilidad de datos, han limitado en algunos casos, las respuestas de salud pública a situaciones de emergencia y los esfuerzos de la subsiguiente vigilancia, al imponer el estricto diseño de base de datos y manejo de requerimientos.

Requerimientos para el manejo de Datos

En investigaciones epidemiológicas, los problemas de enfermedad son caracterizados generalmente por persona, lugar, y tiempo, cuando el problema concierne la emergencia de una enfermedad nueva, un cambio en el modelo de resistencia de un patógeno conocido, una respuesta de emergencia al brote, o un programa de vigilancia de enfermedad de rutina. Los principios de reunión, gestión, y análisis de datos son esencialmente los mismos para todo estos propósitos. Los sistemas computados desarrollados para administrar datos asociados con estos problemas deberían observarse como herramientas para la caracterización epidemiológica de patógenos, síndromes, casos, y factores de riesgo. Por lo tanto, la gestión de datos de laboratorio y la información de los sistemas deben ser capaces de manejar datos sobre todo estos aspectos.

Los requerimientos más estrictos para la gestión de datos son impuestos por los datos del laboratorio que analiza especímenes de pacientes, humanos y no humanos, y del ambiente. Un sistema modelo de datos reaccional adecuado a ser manejado adecuadamente será casi ciertamente adecuado para el manejo de los requerimientos de datos clínicos, de exposición y demográficos.

Dos funciones de gestión de datos primarias pueden satisfacer las demandas de datos de laboratorio con requerimientos múltiples en cada función. La primer función, la gestión de datos de internos de laboratorio, consiste en la entrada de resultados y ruta de los especímenes analizados. El segundo, la vigilancia, incluye reunir datos y mover datos más allá de los archivos electrónicos del laboratorio a sitios apropiados para el análisis. Un sistema de gestión de datos debería ser capaz de desempeñar estas funciones no solamente durante un brote sino a lo largo del período de vigilancia también.

La función interna del laboratorio, universalmente similar entre la mayoría de los laboratorios de salud pública, incluye la entrada de datos adaptado para laboratorios individuales en el lugar; la recuperación/capacidad de búsquedas; y la capacidad para agregar o borrar análisis, administrar alícuotas, compartir entrada de datos en laboratorios en diferentes sitios, investigar la condición de cada espécimen sin considerar en que laboratorio fue analizado, desarrollar informes para presentar especímenes, y en algunos casos asignar los costos para las pruebas de laboratorio desempeñadas y preparar facturas para los remitentes.

Las necesidades para la función de vigilancia incluyen, además de ciertos datos críticos de laboratorio, las siguientes instalaciones: registrar datos clínicos, exposición/factor de riesgo, y datos demográficos sobre los pacientes; a incluir los datos sobre las alícuotas y especímenes múltiples relacionadas a la misma persona, sin considerar el intervalo que separa las fechas de espécimen; y cambiar preguntas o resultados de análisis que se registran para cada espécimen.

Aunque las funciones internas y de vigilancia están claramente separadas, no son independientes. Los datos ingresados en las bases de datos para la función interna deberían estar disponibles sin esfuerzo adicional para la función de vigilancia. De hecho, cuando la función interna no es electrónica o cuando el sistema electrónico interno es inadecuado, el sistema que desempeña la vigilancia electrónica debería desempeñar también en alguna extensión las funciones internas. La buena gestión de datos de laboratorio no llevan a cabo la función interna en exclusión de la función de vigilancia.

Si un sistema de gestión de datos de laboratorio será útil para situaciones de emergencia, debe brindar mecanismos para adaptase rápidamente a la situación de emergencia. Por ejemplo, debe brindar una manera para inmediatamente crear un instrumento electrónico de recolección de datos y para incorporar este instrumento nuevo en el sistema en todos los sitios de informe electrónicamente. Para la función de vigilancia, estos aspectos electrónicos deben incluir instalaciones de comunicaciones para mover datos electrónicamente desde una ubicación a otra, mecanismos para archivos o mensajes remitentes, funciones para el análisis simple, y métodos para preparar e imprimir informes. Mientras algunos sistemas desempeñan algunas de estas funciones, la mayoría de los sistemas no proveen de todos ellos.

Con sistemas apropiados en mano, los planes de gestión de datos para ambos eventos urgentes y de rutina pueden acercarse en una tendencia secuencial. Con el consenso entre todos los investigadores participantes, los epidemiólogos deberán decidir qué datos (tanto de laboratorio y epidemiológicos) son necesarios de modo que las características del campo de datos puedan definirse. El consenso debería alcanzarse en la fase inicial de la investigación del brote; de otra manera los participantes en la investigación comenzarán la gestión de datos ad hoc en el manejo de sistemas.

En un sistema bien diseñado, las definiciones iniciales en una situación de emergencia pueden incluir proyecciones respecto de cuales datos de campos se necesitarán. Sin embargo, para la vigilancia de rutina estos pueden planificarse más completamente. Así, el sistema de datos debería permitir a los campos borrarse si no se necesitan y de agregarse si llegar a ser importantes. Estas modificaciones deberían 1) manejarse sin tener que alterar el sistema, 2) usar un menú simple de las funciones requeridas sin intervención de un programador, 3) realizar los cambios inmediatamente, 4) distribuirse a todos

los investigadores sin desorganizar sus otras funciones durante la investigación, y 5) incorporarse automáticamente.

Luego, todos los participantes conocidos en la investigación deber identificarse. Estos deberían incluir funcionarios federales, estatales, y locales así como también participantes privados o académicos quienes pueden brindar informes al depósito central de datos. Estos participantes deben identificarse al sistema específicamente por la persona y por el sitio para la seguridad de sistema. Las oficinas del estado y federales apropiadas deberían informarse en lo que concierne al sistema computado y las reglas para su buen uso antes de que una emergencia ocurra; por lo tanto, los sitios estarán en el sistema por adelantado de un problema urgente. Sin embargo, el sistema debe permitir que nuevos sitios se agreguen rápidamente. En una emergencia, un acuerdo temporario debe concretarse para todos los participantes para colaborar con las demandas de la situación, p. ej., para usar un sistema particular de software y operar bajo un conjunto estándar de reglas para recolectar datos de informes en una emergencia. Este acuerdo puede estipular ocasionalmente que los participantes compartan datos temporalmente en una base de datos común en aras de la integridad de los datos.

Entrando sobre los mismos casos en la misma base de datos los datos clínicos, factor de riesgo epidemiológico, y de laboratorio, más que combinando bases de datos separadas después que los datos se recolectan, brinda grandes retribuciones en integridad de datos y ahorra tiempo que el esfuerzo de obtener cooperación para una base de datos común durante una situación urgente es útil. Aunque combinando bases de datos múltiples durante la vigilancia de rutina es factible, que las situaciones de emergencia no prestan a sí mismos a este tipo de gestión de datos. Por lo tanto, el sistema a ser usado para estas situaciones debe acomodar una base de datos común y brindar un medio de conección de los sitios de informes a la base de datos. Cuando el sistema de informe es activado y los datos comienzan a llegar a un lugar central, el sistema debería facilitar el análisis en cada sitio de informe y brindar un mecanismo para exportar datos (p. ej., archivos ASCII o dbf) para el análisis externo.

Las situaciones de emergencia crean demandas inusitadas para los recursos de laboratorio y epidemiológicos; por lo tanto, la gestión de datos no debería desorganizar o amenazar desviar recursos dedicados a estos otros propósitos. Como el sistema se implementa, antes de la ocurrencia de las emergencias, las discusiones de los recursos requeridas deberían tener lugar con los participantes. Los participantes deben dedicar algunos recursos a la gestión de datos, pero estos deberían minimizarse. Este es consistente con implementar un sólo sistema a principios del brote de investigación y continuando con el seguimiento de vigilancia de rutina. Incorporar los datos en un segundo sistema para la vigilancia podría derrochar recursos.

Aunque la gestión interna de datos no necesita que cambie para acomodarse a un brote, los laboratorios deben implementar sistemas que puedan alimentar directamente datos en el sistema de base de datos maestro, o mediante una función de importación contenida en el sistema maestro o por una interfase directa entre el sistema interno de laboratorio y el sistema de informe de vigilancia.

Las consideraciones sobre gestión de datos durante la investigación y vigilancia del brote en los Estados Unidos incluye los intereses políticos de los participantes. Las limitaciones legales y políticas de todos los participantes deben tratarse antes que la necesidad de tratar con ellos crezca. Sobre una escala global, esta consideración es igualmente importante, especialmente en países cuyas economías pueden ser adversamente afectadas por noticias de una situación peligrosa de enfermedad. La soberanía individual de país no debe ser violada por informes de datos, y la cooperación de cada país participante o la entidad política (p. ej., la organización Mundial de la Salud (WHO), Organización panamericana de Salud (PAHO)) debe obtenerse en una atmósfera de confidencialidad. Todo los intentos de obtener, compartir, o combinar datos sobre una base global o regional deben incluir un buen definido conjunto de reglas acordadas por todos los participantes. Por ejemplo, los datos para propósitos científicos podrían recibirse en una oficina de la WHO o PAHO pero no enviados más allá de estas organizaciones.

La mayoría frecuentemente, en aras de la vigilancia sobre una escala global o regional, las consideraciones de gestión de datos deben enfocarse primero en establecer en el país infraestructuras de gestión de datos. Esto significa que la vigilancia global o regional primero se traducirá en establecer un sistema maestro, o sistemas por lo menos compatibles con los países individuales participantes. En la mayoría de los casos, los sistemas de gestión de datos disponibles en los países en desarrollo no brindan el modelo correlativo necesitado por el laboratorio. Por lo tanto, los esfuerzos deberían ser iniciados para introducir y establecer sistemas que puedan encontrar estas necesidades en países que desean que los usen.

Un plan para la vigilancia global o regional debe incluir herramientas para responder a brotes y brindar el equipamiento de computadoras y modem u otros medios de transmitir los datos electrónicamente. El ambiente actual demanda que la mayor parte del manejo de datos sea realizado sobre computadoras personales

ubicadas en sitios críticos donde los datos puedan ser ingresados. Sin embargo, el volumen de datos puede requerir finalmente que el sistema facilite archivar datos en otro medio. Esto no excluye el uso de computadoras personales para la gestión de datos pero simplemente reconoce que la tecnología actual limita el volumen de datos que pueden prácticamente ser administrados y analizados en computadoras personales.

El plan inicial de gestión de datos para un país debería incluir una sección sobre procedimientos de informes y el medio apropiado para archivar datos. Para manejar una situación urgente inmediata el sistema debería contener, en un mínimo, una computadora personal con un disco duro de gran capacidad (por lo menos 1-2 gigabytes en el nivel central y posiblemente 300-500 megabytes en cada sitio de informe), gran memoria (por lo menos 4 megabytes de RAM en cada sitio de informe), velocidad adecuada (por lo menos 33 megahertz en cada sitio de informe), y modem rápidos si es posible. Para sitios ubicado en áreas con líneas inadecuadas de teléfono, otras formas para transmisiones electrónicas deberían planificarse (p. ej., disquetes). Hasta que la seguridad pueda asegurarse en Internet, nosotros no recomendamos usar este medio para la transmisión electrónica de datos clínicos de laboratorio para los brotes de investigación y vigilancia.

Nuevas herramientas para la Gestión de Datos de Laboratorio

Sistema de Vigilancia de salud pública (Public Health Laboratory Information System) (PHLIS)

Para conducir las necesidades de un sistema de gestión de datos para investigaciones y vigilancia de brotes, el National Center for Infectious Diseases, CDC, en cooperación con los directores de Laboratorios de Salud Pública y la Association of State desarrollaron el PHLIS. Con este sistema, las pantallas de entrada de datos (los módulos) se crean y distribuyen a todos los sitios de informe electrónicamente, y los datos son ingresados e informados en horas, sin involucrar programadores de computadora. PHLIS brinda la capacidad para un plan de informes jerarquizados que involucra informes a múltiples niveles de informe consecutivamente más altos; una base de datos se crea en cada nivel de informe de modo que todos los datos informados al sitio o el aporte en el sitio se incluyen en la base de datos en ese sitio.

La versión más reciente de PHLIS (Versión 3.0), es un sistema menú-conducido con base en datos correlativos que modelan suficiente para las necesidades planteado en la primera parte de este informe. El sistema permite un registro para un paciente a ser ingresado sólo una única vez y vincula especímenes múltiples para ese registro de paciente. Estos es cierto aun cuando los especímenes para el mismo paciente son ingresados en módulos diferentes de enfermedad, o si el nombre del paciente será agregado en un módulo que contiene sólo datos epidemiológicos (no especímenes de laboratorio). PHLIS provee un conjunto de núcleo de datos a ser recolectados en cada paciente. Además, cada módulo de enfermedad puede ser personalizado agregando campos adicionales a los datos del núcleo si es necesario. El sistema puede acomodar datos para estudios epidemiológicos, laboratorio, encuesta, y caso-control, y para otras necesidades salud pública.

El personal de campo puede agregar rápidamente sus campos de datos propios a módulos existentes de enfermedad para personalizar la entrada de datos para necesidades especiales en cada sitio de información de datos. Durante un brote, un nuevo módulo puede rápidamente desarrollarse y ser electrónicamente transmitido a todos los sitios participantes del informe.

El sistema, que incluye el software de comunicación de datos, se configura de modo que los datos fluyen en una estructura de informe piramidal: esto es, los datos se informan desde el nivel más bajo hacia sitios de nivel más alto y finalmente al sitio central único. Como los datos se pasan a un nivel consecutivamente más alto, éstos se asimilan automáticamente en la base de datos de ese sitio. Así, las bases de datos se construyen y son actualizadas en sitios de informe consecutivamente más altos. Información adicional sobre un caso o espécimen puede agregarse en cualquier sitio de informe; si se desea, estos datos adicionales se transmiten también al próximo sitio de informe más alto. Para hallar la necesidad de retroalimentación, PHLIS tiene un opción en el menú-conducida para transmitir archivos o mensajes arriba y abajo de la cadena de informe, con estos archivos y los mensajes siendo transmitidos automáticamente cuando se establecen conexiones para cada transmisión de datos. Esta facilidad es lo suficiente flexible para permitir a cualquier usuario valedero en la cadena de informe transmitir archivos o mensajes a cualquier otro usuario en la cadena de informe. Por ejemplo, en los Estados Unidos, un funcionario de salud de un condado que esté incluido en el sistema de informe en un estado puede enviar mensajes o archivos al funcionario participante del condado en otro estado. El sistema de retroalimentación no simula el correo electrónico porque estos archivos y mensajes son enviados a lo largo de la cadena de información en la misma configuración de comunicación de informe de datos. Por lo tanto, la llegada exitosa de estos mensajes en su destino (s) depende de cada miembro de la cadena de información entre el remitente y el receptor para establecer una conexión para propósitos de información. Sin em-

bargo, el sistema brinda un mecanismo alternativo para los mensajes y archivos remitidos directamente a cualquier otro informador teniendo capacidad para recibir sin ir a través de la cadena de información.

PHLIS es usado en todos los 50 laboratorios estatales de salud pública, así como también el Distrito de Columbia y Guam. Los módulos de enfermedades incluidos son rabia animal, Campylobacter, *Escherichia coli* O157:H7, Enfermedad de Lyme, micobacteria, virus respiratorios y entéricos, Salmonella humana, *Salmonella* no humana, *Shigella*, y droga-resistente a *Streptococcus pneumoniae*.

PHLIS puede implementarse independientemente: las organizaciones pueden desarrollar sus propio sistema de informe piramidal PHLIS. Por ejemplo, el PHLIS actualmente está siendo implementado en el Caribbean Epidemiology Center (CAREC) en Trinidad y en sus países miembros para informes de HIV/infecciones ETS, con la expectativa que el sistema de informe se expandirá a otras enfermedades. CAREC puede recibir informes desde los países miembros en la medida que cada país sea agregado a la estructura de información.

Sistema de Información de Rastreo de Laboratorio (LITS)

El segundo sistema, LITS (Laboratory Information Tracking System), es un sistema basado en PC (Computadora Personal) en un área de red local para el registro de muestras de laboratorio. El sistema permite que la información de la muestra sea ingresada en un sitio central que recibe el espécimen; información adicional sobre el espécimen puede entrarse en el sistema en cualquiera de los laboratorios que realizan pruebas sobre esa muestra. Aunque los módulos son personalizados para las necesidades de cada laboratorio, los laboratoristas pueden agregar pruebas adicionales o borrar las obsoletas. Además, los usuarios pueden examinar todos los datos acerca de un espécimen, incluyendo datos desde todos los laboratorios que desempeñaron pruebas sobre el espécimen. Otros aspectos en el sistema incluyen facturación de costos, informes definidos por el usuario, búsquedas definidas por el usuario, y rastreo de muestras o pacientes y seguridad. Para las enfermedades emergentes, LITS brinda un mecanismo para normalizar protocolos de laboratorio a través de organizaciones y un mecanismo para compartir datos sobre de especímenes dentro de una organización.

Agradecimientos:

Agradecemos a Tim Kuhn por la conducción del equipo programador; Bruce Wilson, Dana Crenshaw, Joe Bates, y Neil Jones por el apoyo de programación; Tim Day por el apoyo usuarios; Kathleen Maloney, Joy Goulding, Lori Hutwagner, y Cecile Ivey por evaluar la integridad del programa; Brian Plikaytis por involucrarse inicialmente con LITS; y Cheryl Shapiro por el manejo financiero.

Referencias

1. Fraser DW, Tsai TR, Orenstein W, Parkin WE, Beecham HJ, Sharrar RG. Legionnaires' disease: description of an epidemic of pneumonia. N Engl J Med 1977;297:1189-97.
2. Shands KN, Schlech WF III, Hargrett NT, Dan BB, Schmid GP, Bennett JV. Toxic shock syndrome: case-control studies at the Centers for Disease Control. Ann Intern Med 1982;96:895-8.
3. CDC. Outbreak of acute illness southwestern United States, 1993. MMWR 1993;42:421-4.
4. Administrative Conference of the U.S. Privacy Act. In: Federal Administrative Procedure Sourcebook, 2nd ed. Office of the Chairman, 1992:863-979.
5. Administrative Conference of the U.S. Freedom of Information Act. In: Federal Administrative Procedure Sourcebook, 2nd ed. Office of the Chairman, 1992:633-61.