

Survey of BT Directors on Legal, Confidentiality and HIPAA Issues in Syndromic Surveillance

National Syndromic Surveillance Conference

October 24, 2003

James Gibson and Dan Drociuk

South Carolina Dep't. of Health and
Environment

HIPAA Privacy: Other Permitted Disclosures (164:512)

1. Required by law
2. Needed for **public health activities** -
Surveillance, investigation, prevention activities, partner notification, vital statistics
3. Avert a serious threat to health or safety
4. Research
5. Others

If syndromic surveillance is public health, then it is permitted by HIPAA!

De-Identified or “Limited” Data Can be Disclosed

- Remove all of the 18 individual identifiers
- Can keep one or more of the 18 identifiers **only if** a statistician determines people can't be identified
- Create “**limited data set**” (PHI with identifiers of pts., relatives, employers removed.) Requires data use agreement

Specific Identifiers

1. Name
2. All address info
3. E-mail addresses
4. Dates (except year)
5. SSN
6. Medical record number
7. Health Plan beneficiary number
8. Account numbers
9. Certificate numbers
10. License numbers
11. Vehicle identifiers
12. Facial photos
13. Phone numbers

Specific Identifiers

14. Device identifiers

15. URLs

16. IP addresses

17. Biometric identifiers

18. All geographic subdivisions below state except for first three digits of ZIP code (if over 20,000 population)

Methods

- **Sept-Oct:** Joined teleconference discussions to brainstorm potential issues
- **Oct 3-9:** Developed and piloted a 9-question survey instrument
- **Oct 15:** Survey emailed to 52 state/city CDC Bioterrorism “B” directors and 51 state epidemiologists
- Requested forwarding to city/county systems
- Permitted anonymous reporting of responses
- **Oct. 17-22:** 32 responses received

Response to Survey, by 10/21

- 34 jurisdictions submitted a response
 - 27 states, 6 cities/counties, 1 territory
- ≥ 10 states/major cities with known systems did not reply (at least)
- 6 requested anonymous reporting, 8 did not respond

Results: Question 1

- Currently not considering SSS*: 3 (9%)
 - Considering or planning SSS: 8 (24%)
 - Implementing, and recruiting: 6 (18%)
 - Running a SSS: 17 (50%)
-
- Not representative of all states

* SSS=Syndromic surveillance system

Question 2: Stories (summaries)

“Few problems” n=11

- Not especially difficult problem. Key is with whom you talk in the hospital re pt. F/U. Long established relations with ICPs (CT)
- SSS collects aggregate data only. Very few asked about HIPAA. Provided HIPAA training to hospitals (MO and several others)
- We relayed the MMWR on HIPAA with further info on state regulations: no major problems
- We limit data to date/time, demographics, CC, Dx, disposition, zip codes. “Limited data set”=no tracking
- Has occurred rarely, resolved by discussions w admin
- Collect no identifiers. But IRB approval was required

Question 2: Stories: “Significant problems”

- System developers had to reassure hospital Risk Managers, and agreed to de-identify data. (NC)
- Even our routine investigations encountered roadblocks. Many people in the trenches don't know enough about HIPAA. Do not give info beyond “minimum necessary”. Hampers disease surveillance also. (OR)
- We developed a data use agreement that addresses these concerns. Substantially restricts distribution of data.
- Almost every hospital we approach has raised issue of compliance with HIPAA. Discuss “minimum data set” method, and are now citing a recently passed state law.
- Imagined concerns are very real, providers require additional review and approval stages

Qu. 2: What has been your experience with confidentiality and HIPAA in SSS?

(N=23)

- Substantial problems: 3 (13%)
 - Some problems: 9 (39%)
 - No problems: 11 (48%)
-
- But at least 11 jurisdictions reported they collect only aggregated or significantly de-identified syndromic data. “Significantly” = could not identify case causing a “signal.”

Question 3: “Syndrome reporting is not mandated like disease reporting”

- Yes: 16 (52%)
 - No: 14 (45%)
 - Other 1 (3%)
-
- Disease reporting is considered more accurate, so doctors feel SSS is unnecessary. Education was effective in most cases.
 - There is a clear JCAHO and HRSA incentive.
 - Issue more of astute clinician vs syndromic srvl

Question 3b: “Considered adding SSS to state reporting statutes?”

- Yes 11 (35%)
 - No 20 (65%)
-

- Promulgated a Rule that requires electronic reporting of CC data. By 11/1/03 hospitals must submit plan for compliance. (MO)
- The way in which we presented the system made each hospital a partner in looking for unusual illness. Also automated process to make it more acceptable.
- Not until more evaluation has been done to understand the value of SSS

Question 4: Issues from HIPAA-required “tracking” of disclosures

- Yes 7 (24%)
 - No 21 (72%)
 - Not sure yet 1 (4%)
-
- No, however our system keeps an audit of access by PH to reported patient records.
 - Not so far, but our electronic data exchange may constitute a record.
 - We tell sites that info is a “limited data set.”
 - Misconception re “routine accounting” and its not clear who has the authority to correct this misinterpretation
 - Issues of feasibility and cost of tracking

Question 5: Issues from need to investigate “signals?”

- Yes 8 (26%)
 - No 17 (59%)
 - Other 4 (15%)
-
- Investigation of flags quickly showed that we need individual patient records to trace information
 - We were told the facility didn't deem it necessary since extra cases were in one family
 - We evaluated/revised flagging system..to reduce the number of unnecessary follow-ups
 - Fairly informal follow up locally. As we define the “whens” better, we anticipate more issues will arise.

Question 6: Concern that participation would create bad public perception of hospital?

- Yes 0
 - No 30
-
- It has been quite the opposite: hospitals want to participate, reflects their commitment to community.
 - Hospitals like the daily ED visit summaries.

Question 7: Other legal issues?

- Yes 2 (7%)

- No 28 (93%)

- We've found it's important to get the right people at the table when presenting SSS to a new hospital.
- Yes, there are issues of competitive data being available to other area hospitals if he reports were made public.
- So far we have been able to secure participation without legal data sharing agreements.
- At state, we call ourselves Business Associates. But if asked to sign a BA agreement, we must submit to legal

Question 8: Concerns re providers' costs, or of "unfunded mandate."

- Yes: 11 (35%)
 - No: 20 (65%)
-
- Initially c/o re staff time involved. Hospitals get funds from BT. Fewer c/o after on-line data entry and our sharing data analyses.(CT)
 - Costs are huge issue. ICPs are feeling squeezed.
 - We pay for data access and programmer time.
 - We spent time to actually speak to the sites, and make changes to address their issues.

Question 8b: How are hospitals' costs paid for

- We provide minimal development support for pilots. This is a relatively inexpensive project.
- We explained what would be needed. Hospital Assoc has HRSA grant to offset those costs (MI)
- We use a “low cost data sharing setup,” simple file formats, and say SSS will benefit their county.
- We pay entire cost, with contractor to install interface using fed. Funds. Also made it a condition for receiving HRSA BT funding
- Providers recognize benefits to them, but their IT see it low priority, are slow to write data extraction programs

Question 9: Concerns about adequate data security?

- Yes: 5 (17%)
 - No: 25 (83%)
-
- With the HESS, this issue has surfaced.
 - Security is always an issue, and is one of the first handled by our IT staff. Analytic staff has no access to the “real” database, only a copy.
 - Those concerned use encryption provided by us
 - It is everybody’s biggest concern. Biggest challenge
 - Our SSS is part of regular disease reporting with which ICPs are very familiar. EDs like seeing the lock icon.

Conclusions

- 1. Certain of our hypothesized issues have not been problems in reality: e.g. bad public perceptions from SSS participation;
- 2. Some states have had to deal with confidentiality concerns by significantly limiting the amount of useful identifying data they could collect.