rchn
community health foundation

IT Systems Considerations for Safety-Net Disaster Preparedness

David Hartzband, D.Sc.

Director, Technology Research

RCHN Community Health Foundation

Overview

- Natural disasters and other public health emergencies pose unique challenges for healthcare safety-net organizations.
- During and following a disaster, community health centers, along with other safety-net organizations, must be prepared to provide continuity for existing patients, while addressing triage and emergent needs of community members.
- Maintaining business and clinical operations in a disaster scenario requires deep and ongoing preparation, redundant technology and effective communication to optimize services even when infrastructure fails.
- The presentation will briefly review relevant regulations, and examples will be used to illustrate effective preparation, risk -assessment approaches and responses that optimize resilience for recovery. Participation from attendees will also be encouraged.

Presentation Outline

- The hard truth: **Planning is hard, but it is easier than recovery without planning!**
- General Considerations
- Hardware & Network
- Data
  - What Data
  - Data Access
  - Data Recovery
  - Data Quality
- Applications
  - EHR & Other
- IT Process Review
- This presentation is only about **IT considerations** – other areas such as water supply, clinical supplies & medicine supply are just as important in maintaining continuity of care after a disaster

CMS Emergency Preparedness Requirements for Medicare and Medicaid Participating Providers and Suppliers (effective date 11/25/2017)

- Risk Assessment and Emergency Planning (Include but not limited to):
  - Hazards likely in geographic area
  - Care-related emergencies
  - Equipment and Power failures
  - Interruption in Communications, including cyber attacks
  - Loss of all/portion of facility
  - Loss of all/portion of supplies
  - Plan is to be reviewed and updated at least annually
- Communication Plan
  - Complies with Federal and State laws
  - System to Contact Staff, including patients' physicians, other necessary persons
  - Well-coordinated within the facility, across health care providers, and with state and local public health departments and emergency management agencies.
- Policies and Procedures
  - Complies with Federal and State laws
- Training and Testing
  - Complies with Federal and State laws
  - Maintain and at a minimum update annually

General Considerations - IT

- Again - Planning is hard, but recovery without planning is **much** harder, maybe not possible!
- First step - complete an up-to-date inventory of hardware and software including: vendor, license details, version(s), primary & backup locations, accessibility & security details (with personnel responsible)
- Second step - create backup and recovery plan for hardware & software
- Third step - put processes in place to maintain & evolve inventory, backup & recovery plans as well as drill for recovery
- Planning is not just for line staff – People at all levels of the organization must be aware of & involved in disaster planning!

The Bottom Line at the Beginning…

- Everything must be replicated
  - Hardware, software, data – everything.
- Planning is about setting up this redundancy, determining what is needed, establishing how to test it & understanding how to access it
- Replication must provide:
  - Alternative network provision with live switching
  - Servers (can be virtual) that are either live or updated often so that they can be switched to when necessary
  - Live or recently updated data sources for strategic data (EHR, financial…)
- Replicates should be located off-site, in a separate and secure location so that they are less likely to be affected (virtual or cloud-based)

Electrical Supply

- Almost all recovery efforts depend on a stable & uninterrupted supply of electricity.
- Electrical interruption should be planned for by the installation of a generator system. A consultant or specialist should be used to size the power requirements appropriately & select the correct generator or generator system. Power requirements should be decided on by the health center (should all power needs be covered?)
    - A solar energy system may also be feasible (depending on climate). This also needs careful planning so that adequate power is available.
- Once installed, the system including supply switch-over, should be tested at regular intervals – just having the generator does not guarantee a usable electrical supply.
    - An adequate fuel supply must be arranged for as well

Hardware & Network, etc…

- How is the network provided? Private service line (T1, T3, etc.)? Are there alternatives in place? Public internet? ISP? Etc. Can service be switched to the alternative? Has it been tested?
- Are servers located on premises? Are there alternate servers on or off premises that are mirrored & can be switched to?
- Are servers virtual? Are there duplicates that are regularly updated? Is there a set of duplicated virtual environments on or off premises that can be used?
- Does EHR vendor provide cloud-based service that can be accessed from alternative devices?
- Do other software vendors (financial, etc.) offer cloud-based services? What recovery capabilities do other vendors provide?

➢The goal is to provide a duplicate set of systems that are either cloud-based or remotely located that can be used in case of interruption of operations for whatever reason.

Data? What Data?

- Most CHCs and other safety-net organizations have ~5-10 GB of data total
- PCAs might have 35GB-50GB, Kaiser Permanente has ~45 Petabytes
- Data ranges from clinical, demographic, patient financial, insurance, cost accounting, inventory & ordering, logistics, public & population health, etc., etc…
- All of this data has to be accounted for in disaster planning and in disaster recovery – A person needs to be responsible for ensuring this (& there needs to be a back-up for that person)
- First step is to have a complete data inventory (as complete as possible): where is it located? how is it accessed? is it backed up? Is the backup accessible? Is this information available in a non-electronic form (partially on paper)? Who knows about it?

Data Accessibility

- Inventory should locate all data and specify access paths & processes
  - Are critical data sources (EHR, financial…) only accessed through their application or are their alternative paths (*e.g.* SQL query direct to underlying data store or to a data warehouse)
- Paths to all data sources, including alternative sources should be periodically tested
- As soon as possible after service interruption, access paths for all existing data sources should be tested & data accessed if possible

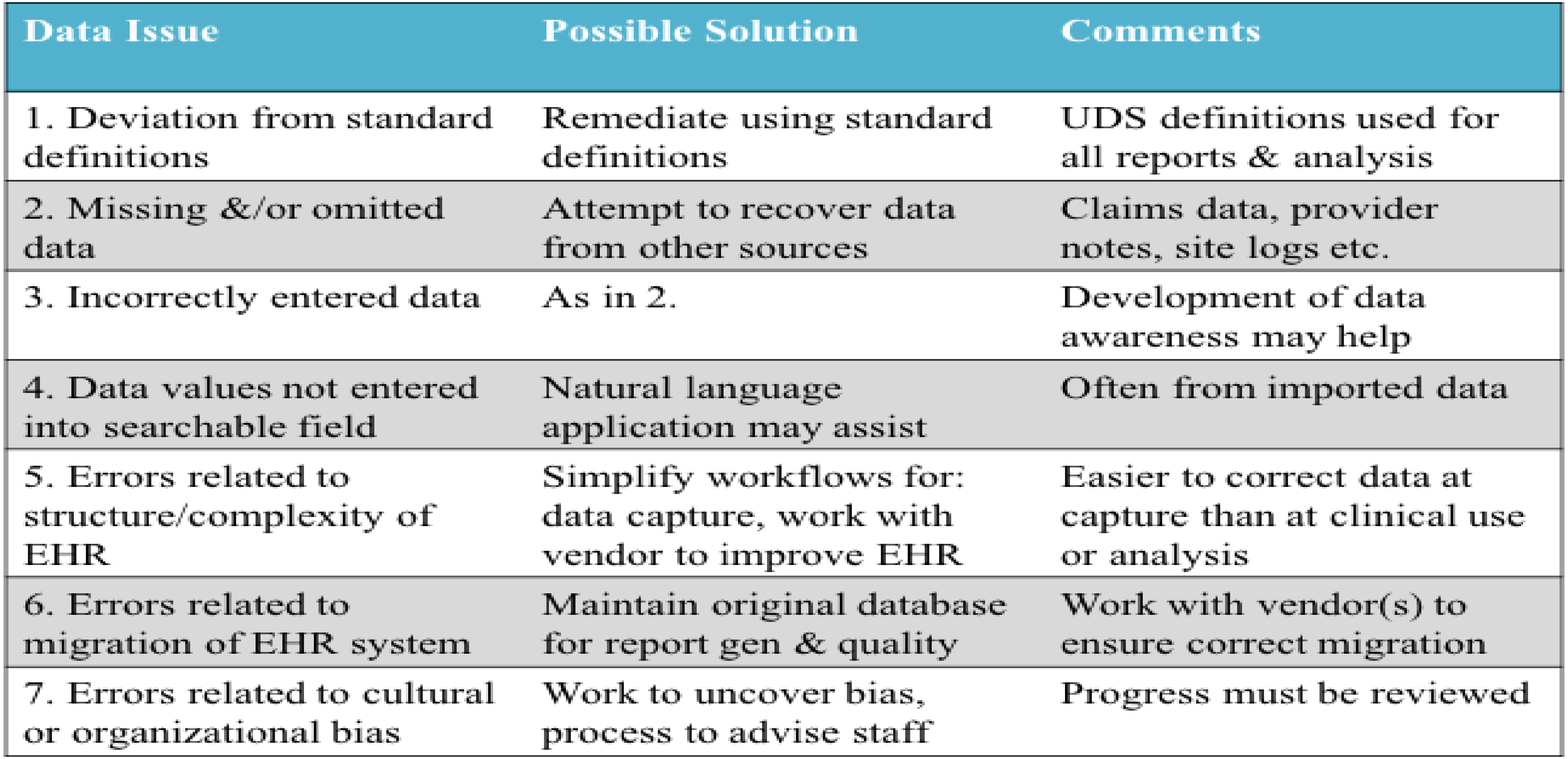
Data Recovery

- As soon as possible after the event, data access paths to alternate data sources should be executed and data flow restored. This may involve using alternate hardware at remote sites, or local hardware that has had function restored. If neither of these alternatives is possible, and data from mirror sources (usually virtual) is accessible, function might be restored on new &/or shared (borrowed) hardware
  - If no mirror source is available, data must be restored from local or remote physical or virtual sources
  - If data backup is not available, data flow should be established as soon as possible with live data while other recovery strategies are pursued
  - Some examples might include: restoration of clinical & demographic data from 1) claims data (on demand, possibly through clearinghouse if one is used) 2) secondary source such as HIE or HCCN data warehouse (please note: this could be a primary recovery strategy) 3) other
- Assume that the EHR will not be available – develop and print paper forms for encounters so that data can be recorded by providers (& other staff). Enter data from forms when EHR is available again.

Data Quality

- Disaster-based service interruptions will cause data quality issues
- Data entry is interrupted & may not resume at scale for some time
  - Alternate data entry (paper) methods may be used for a period & this data will need to be entered into the restored system to ensure continuity
- Data in alternative sources sources may have issues with missed or missing updates
- Data recovery efforts may cause corrupted &/or missing data
- Data quality testing must be done, ideally on alternative sources before restoration, but certainly after restoration
- Amelioration of data issues may be possible (see next slide…)

Data Quality Issues & Corrections



Data Issue	Possible Solution	Comments
1. Deviation from standard definitions	Remediate using standard definitions	UDS definitions used for all reports & analysis
2. Missing &/or omitted data	Attempt to recover data from other sources	Claims data, provider notes, site logs etc.
3. Incorrectly entered data	As in 2.	Development of data awareness may help
4. Data values not entered into searchable field	Natural language application may assist	Often from imported data
5. Errors related to structure/complexity of EHR	Simplify workflows for: data capture, work with vendor to improve EHR	Easier to correct data at capture than at clinical use or analysis
6. Errors related to migration of EHR system	Maintain original database for report gen & quality	Work with vendor(s) to ensure correct migration
7. Errors related to cultural or organizational bias	Work to uncover bias, process to advise staff	Progress must be reviewed

Applications – EHR, etc.

- Vendor contracts should include provisions for restoration &/or replacement of critical application software (EHR, PMS, PopHealth, Registries etc.) following a disaster
- Vendors may also be able to help with data recovery
  - Provide backup & recovery functions for their app
  - Provide data aggregation &/or warehousing function
- Applications such as EHRs may be able to be utilized even without an electrical supply so long as the data and software is available in the cloud, and a device like a tablet is used as the interface. Such devices may be able to be recharged from vehicles.

Example – Access Family Care, Joplin MO

- On May 22, 2011 at 5:41pm an EF-5 tornado (200mph winds) struck Joplin Mo causing extensive damage including: 8,000 properties & 19,000 vehicles destroyed, ~$3B in damages & 162 tornado related deaths
- Access Family Care (AFC), a FQHC in Joplin, is part of the city's disaster planning group & actually had a person in the city's Emergency Ops Center on May 22.
- Learning from previous disasters, AFC planned as part of its transition to an EHR, to work with a vendor that could provide off-site secure hosting & access from almost any device.
  - They also planned to use pre-printed paper forms for encounters if the EHR was unavailable.
  - They also had plans for uninterruptable electrical service & water use. Fortunately, their primary clinic never lost power

Example – AFC… continued

- Patients started arriving almost immediately following the all clear. AFC started by using their pre-printed paper forms which were entered into the EHR as soon as it became available
- Patients continued arriving until about 2am. AFC opened at 8am as usual on May 23rd.
  - Access initiated the delivery of tetanus vaccine & administered ~2000 doses following the incident
  - Access personnel went out into the community & did triage & treatment
- For a deeper look at AFC's planning & reaction to this disaster see:

Shin & Jacobs, 2012 - https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3615799/

IT Process Review

- Critical IT processes should be reviewed and tested at least twice a year – This review needs to be under the supervision of an Executive Staff member & have specific other personnel responsible for relevant pieces
- This review should include:
  - “tabletop” review, that is working through a disaster scenario on paper using current processes (once a year)
  - Testing all alternative switching: network, servers and data access (once a year)
- After testing, issues should be discussed and modifications made to plans & processes as necessary
- Plans/processes should be documented and documents updated after each test
  - Documentation and maintenance needs to be the specific responsibility of a staff member
- There should also be a plan for post-disaster process review as necessary

Lessons Learned

- Disasters are not predictable. Another tornado in Joplin, MO would be a different event & possibly require a different response. So would another hurricane in Puerto Rico or anywhere else.
- Planning cannot be perfect, but can be comprehensive enough to allow for an effective, flexible response.
- People must have well-understood roles and well defined processes to execute
- When a disaster occurs, response must start as soon as possible with whatever tools are available
    - Assume that resources like water, electricity, internet will not be available for much longer than official estimates
- Everything must have multiple redundancies & locations
- Partners, including state and municipal agencies, regional healthcare organizations, IT & logistics vendors, local hospitals and other healthcare practices etc. are very important. Relationships need to be established & maintained so that “mutual aid” can be delivered
- Personnel on the ground must be familiar enough with processes & resources that they can react & adjust operations as needed

rchn
community health foundation

?

David Hartzband, D.Sc.

Director, Technology Research
RCHN Community Health Foundation

dhartzband@rchnfoundation.org
617.501.4611