Pandemic influenza and critical infrastructure dependencies: possible impact on hospitals

Ralf L Itzwerth, C Raina MacIntyre, Smita Shah and Aileen J Plant

ABSTRACT

- Hospitals will be particularly challenged when pandemic influenza spreads.
- Within the health sector in general, existing pandemic plans focus on health interventions to control outbreaks.
- The critical relationship between the health sector and other sectors is not well understood and addressed. Hospitals depend on critical infrastructure external to the organisation itself.
- Existing plans do not adequately consider the complexity and interdependency of systems upon which hospitals rely. The failure of one such system can trigger a failure of another, causing cascading breakdowns.
- Health is only one of the many systems that struggle at maximum capacity during "normal" times, as current business models operate with no or minimal "excess" staff and have become irreducible operations. This makes interconnected systems highly vulnerable to acute disruptions, such as a pandemic.
- Companies use continuity plans and highly regulated business continuity management to overcome process interruptions. This methodology can be applied to hospitals to minimise the impact of a pandemic.

MJA 2006; 185: S70–S72

In the late 1990s, hospitals were looked at collectively as organisations under threat, because of the Y2K problem,[1] which had the potential to affect the operation of core computerised systems and cause havoc with all machinery based on or connected to computers and microchips. Massive investment in new computer equipment was the overall response to this threat, and in the event few systems malfunctioned.

As an acute global threat, pandemic influenza is different in many respects: its arrival date is uncertain and it is not organisation-specific, but ubiquitous by definition. It has the potential to affect humans in large numbers over a longer period, possibly months, and its severity is unknown.

Severe acute respiratory syndrome (SARS) showed that health staff were particularly vulnerable and reported sick in large numbers. With pandemic influenza, 30%–50% of hospital staff may not be able to work — some because of illness, some because of competing family responsibilities, and others because of fear.[2] Certain departments of a given hospital with small teams may be completely without staff (eg, the information technology [IT] or accounting departments).

In their pandemic preparedness plans, businesses often assume that a significant proportion of their staff will be unavailable to attend work.[3] For example, the New South Wales Health Services Functional Area Supporting Plan recommends contingency plans for surge staff capacity involving the use of medical and nursing students, retired health care workers, and other groups.[4] However, absenteeism is not the only factor that can affect the availability of external critical infrastructure. For example, a handful of anthrax-contaminated letters in the United States in 2001 effectively shut down the entire US postal service for days, showing that even perceived health threats can cripple infrastructure.[5] In the case of Hurricane Katrina in 2005, police walkie-talkies were rendered useless within hours because the relay stations had run out of power.[6]

Existing hospital-specific disaster management plans address surge response in relation to terrorist attacks and other emergencies.[7,8] However, it is unclear how many hospitals actually have a detailed pandemic or disaster management plan that adequately addresses critical infrastructure. Current pandemic plans focus on health interventions to control outbreaks, and human resource management. Although most hospitals have continuity or disaster plans, our review of these plans has shown that they are not necessarily linked to pandemic preparedness planning.

Large-scale preparations are underway in many countries, at all layers of social organisation from hospitals to councils and businesses, to cope with large numbers of people falling sick or dying from pandemic influenza.[9,10]

Today in developed societies, industry, businesses and other organisations do not operate as isolated entities. Plans need to consider the complexity and interdependency of systems upon which hospitals rely. The failure of one system can trigger a failure of another, causing cascading breakdowns (Box 1). Health is only one of the many systems that struggle at maximum capacity during "normal" times, as current business models operate with no or minimal "excess" staff and thus have become irreducible operations. This makes a system highly vulnerable to acute disruptions, such as a pandemic.

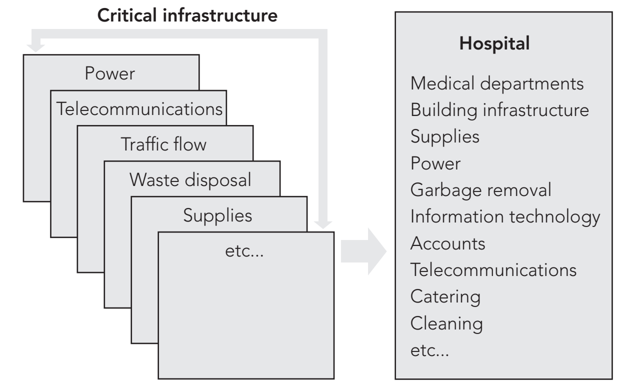
Critical infrastructure

Hospitals, like other organisations, rely on "critical infrastructure" — goods and services that are essential to everybody, which include not only health, but energy, transport, telecommunications, water, emergency services, sewage disposal, and garbage removal (Box 2).

The absence or failure of any of these services can, within a short time, affect entire segments of society or businesses.

Although many hospitals have at least basic plans in place that outline the measures that must be taken if subsystems such as power or water supply are interrupted, these plans assume that such interruptions will be limited in duration and overall effect.[11] For example, diesel generators would have fuel to run them for a few hours, and IT installations would run from special power supplies to prevent data corruption of critical patient databases. Some specialised departments, such as intensive care and emergency, may have dedicated equipment and resources to overcome short disruptions, which are more widely recognised as potential risks and have been catered for by many plans.[12]

1 Interdependency of internal and external systems to hospital functioning



Threats to hospital operations are not the only concern. An outbreak of pandemic influenza could place a substantial economic burden on hospitals, because their normal business would suffer, as was the case when SARS hit the Taiwanese health system.[13] It is also uncertain to what degree insurance would cover any losses.

Business continuity management

Business continuity management and business continuity planning focus on the analysis of risks and the potential effects of such risks on an organisation or business. Business continuity management considers all departments and all business processes, including the input (such as suppliers and essential infrastructure) and output (such as customers, payment and taxes) of the business. As a result of proper business continuity management, a business continuity plan is drafted. This can then be used to manage business interruptions of (theoretically) any type, including loss of core staff or disruption of supplies, which may be caused by the loss of staff at the supplier's organisation. Supply is a more critical issue today than it was during previous pandemics because our economy operates in "just in time" mode more than ever before. This means that most supplies will only last for a very short time, perhaps only days, and there is heavy reliance on a continual chain of supply.

The overall objective of an effective plan is to make a system and its business processes less prone to interruptions, to increase their resilience, and reduce potential downtime. If all these components can withstand minor malfunctions and the organisation or business keeps operating, its degree of resilience or the availability of its components is considered high and the system has a high degree of stability.[14]

A thorough plan would add to these aspects vital components outside the organisation (eg, infrastructure like transport and water, and the resilience of suppliers). Hospitals need to work as part of an integrated plan at state/territory and Commonwealth level. However, some states or territories delegate full responsibility to area health services and hospitals themselves, while others are centrally run.

Applying business continuity management to hospitals and using disruption scenarios for all departments allows the illustration of the potential consequences for the overall functioning of the organisation. Questions remain concerning what could cause any hospital department to become unavailable and what would be the resulting effects for the remainder of the organisation, its staff, and its objective to provide health care services to its customers and patients.

All departments need to be considered under the scenario of a high percentage of staff not being able to attend work, no matter which department or which position. A typical example is accounts payable and salaries: if staff are not paid, they cannot continue their lives; if suppliers are not paid, they will not deliver the supplies. Essential infrastructure services outside hospitals may become unavailable or get disrupted. These include power, telephones, mobile phones, email and paging services, water, and garbage removal.

For a hospital, supplies of food, pharmaceutical products, medical gases and other consumables would have to be added to the "essential" list.

Administration and back office systems

A hospital's departments or subsystems are similar to those of most other businesses: they all have accounting, human resources, and other "back office" systems, like IT, computer networks, telephone exchanges, and building management (which looks after the building's technical systems such as lifts, air-conditioning and security).

Back office systems often escape attention until they fail and their relevance for the functioning of the organisation as a whole becomes evident. This moment of failure of less noticeable machinery and equipment demonstrates another important factor — hardly ever have these systems been chosen and acquired with the resilience of their suppliers or service providers in mind. Usually they have become part of the organisation because they were the cheapest on offer.

It is hardly conceivable that a complex and sensitive structure like a hospital, at a time when it is overburdened with a surge of critically ill patients, could maintain any of its core functions without some or all of the infrastructure services.

Conclusion

Pandemic planning for hospitals and the health sector needs to consider not only health-related strategies, but also the broader systems upon which hospitals depend — both inside and outside the health system. Hospital and health sector pandemic plans need to have designated staff responsible for each critical component of operations, as well as strategies for prioritising resources. They need to integrate their specific requirements with all elements of

2 What is critical infrastructure?

- Hospitals are organisations or systems. As systems, they relate to other systems and depend on them: power supply, telecommunications, water, transport and garbage removal are considered "critical infrastructure".
- Failure of any of these has repercussions for the others: without power we have no phones, no computers, no water pumps, and no lights. Without telecommunications, we do not have control over the power grid or water supply systems.
- All these systems are run by people with specific training and skills. If a significant number of people cannot do their work, the critical infrastructure is at risk, and therefore all organisations that rely on it, including hospitals, are at risk. ◆

3 How to make a hospital resilient: a simple checklist

- Establish criteria for when the business continuity plan should come into effect.
- Arrange backup for individuals and teams and their respective skills; this should include all levels of the hierarchy. Can retired staff be contacted and hired as backup?
- Check the surge capacity for key functions: "copy" scarce skills to other staff. Cross-train staff for essential services.
- Plan to accommodate clinical staff in hotels or other alternative accommodation.
- Provide a communication strategy for staff, and with media and other authorities.
- Communication management: who will review and convey crisis information, and through which media can this be done?
- Identify "essential functions" and how they can be kept functional even if other connected systems have failed.
- Identify departments and services (eg, elective surgery) that could be downsized or closed to free and then reallocate resources.
- Investigate the hospital's ability to continue vital operations if any of the critical infrastructure services become unavailable (eg, work without telephones or computers, or even without power).
- Consider additional security measures that may be needed.
- Ensure training and legal status for reserve health care workers, such as medical and nursing students and retired staff.
- Ensure backup generators are working and have sufficient capacity for several days.
- Have battery-powered phone or other communication systems as a backup for telephone failure.
- Ensure there are stockpiles of drugs, medical supplies and food.
- Prepare contingencies for non-availability of equipment such as ventilators and infusion pumps.
- Plan for emergency garbage disposal services.
- Establish work-from-home connections for departments that can provide service from offsite (eg, accounts, payroll and IT) and mitigate the risk of telecommunication services becoming unavailable.

See http://pandemicflu.gov/ for more checklists. ◆

the supply chain outside their own system, and think beyond the medical-specific approaches on which most current plans appear to focus.

Some resources are specialised for the specific emergency requirements of hospitals,[15] and offer practical training tools. Box 3 provides a simple checklist of factors that hospitals should consider. Securing critical infrastructure is an overarching requirement for all hospitals, and requires a whole-of-government approach.[16]

Competing interests

None identified.

Author details

Ralf L Itzwerth, DipSoz, Sociologist[1]
C Raina MacIntyre, FRACP, FAFPHM, MAppEpi, Professor, Discipline of Paediatrics and Child Health[1]
Smita Shah, MB ChB, MCH, Clinical Senior Lecturer[2]
Aileen J Plant, PhD, MPH, FAFPHM, Professor of International Health[3]

1 National Centre for Immunisation Research and Surveillance of Vaccine Preventable Diseases, The Children's Hospital at Westmead and the University of Sydney, Sydney, NSW.
2 Discipline of General Practice, University of Sydney, Sydney, NSW.
3 Australian Biosecurity Cooperative Research Centre for Emerging Infectious Disease, Curtin University of Technology, Perth, WA.
Correspondence: rainam@chw.edu.au

References

1 Connell R. The impact of the Y2K threat on hospital emergency preparedness. In: Student research accomplishments 2001–2002. Buffalo, NY: MCEER, 2002. http://mceer.buffalo.edu/publications/resaccom/02-SP09/pdfs_screen/16_Connell.pdf (accessed Sep 2006).

2 Wiskow C. The impact of severe acute respiratory syndrome (SARS) on health personnel. Geneva: International Labour Office, 2003. http://www.ilo.org/public/english/dialogue/sector/papers/health/wp206.pdf (accessed Sep 2006).

3 Food industry QRT pandemic analysis: an analysis of the potential impact of the H5N1 avian flu virus. Minneapolis, Minn: CIDRAP, 2005. http://www.cidrap.umn.edu/cidrap/files/47/panbusplan.pdf (accessed Oct 2006).

4 NSW HEALTHPLAN. A supporting plan to the New South Wales State Disaster Plan (DISPLAN). Sydney: NSW Health, 2005. http://www.emergency.nsw.gov.au/media/252.pdf (accessed Sep 2006).

5 Inglesby T, O'Toole T, Henderson DA, et al. Anthrax as a biological weapon, 2002 updated recommendations for management. *JAMA* 2002; 287: 2236-2252.

6 Baum D. Deluged. *The New Yorker* 2006; 9 Jan. http://www.newyorker.com/fact/content/articles/060109fa_fact (accessed Sep 2006).

7 Murnane M, Cooper DM. Is the Australian hospital system adequately prepared for terrorism? The Australian Government's response. *Med J Aust* 2005; 183: 572-573.

8 Rosenfeld JV, Fitzgerald M, Kossmann T, et al. Is the Australian hospital system adequately prepared for terrorism? *Med J Aust* 2005; 183: 567-570.

9 Australian Government Department of Health and Ageing. Australian health management plan for pandemic influenza. Canberra: Department of Health and Ageing, 2006. http://www.health.gov.au/internet/wcms/publishing.nsf/Content/ohp-pandemic-ahmppi.htm (accessed Oct 2006).

10 World Health Organization. WHO global influenza preparedness plan. Geneva: WHO, 2005. http://www.who.int/csr/resources/publications/influenza/WHO_CDS_CSR_GIP_2005_5.pdf (accessed Sep 2006).

11 NSW Health interim influenza pandemic action plan. Sydney: NSW Health, 2005. http://www.health.nsw.gov.au/pubs/2005/pdf/pandemic_ap.pdf (accessed Sep 2006).

12 Australian Government Department of Health and Ageing. Health IAAG — consultancy report. *CIP Newsletter* 2004; 1(3): 2. http://www.tisn.gov.au/agd/WWW/TISNhome.nsf/Page/Publications (accessed Oct 2006).

13 Solomon N. Economic cost to hospitals from an avian flu pandemic likely to be huge, SLU professor says. *SLU Newslink* (St Louis) 2005; 17 Nov. http://www.slu.edu/readstory/newslink/6254 (accessed Sep 2006).

14 Rinaldi SM, Peerenboom JP, Kelly TK. Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine* 2001; 21: 11-25.

15 American Hospital Association. Protecting and improving care for patients and communities. Emergency readiness. 2006 advocacy issue paper. http://www.hospitalconnect.com/aha/key_issues/disaster_readiness/resources/flu.html (accessed Sep 2006).

16 Attorney-General's Department. Emergency management. http://www.ema.gov.au/agd/EMA/emaInternet.nsf/Page/Emergency_Management (accessed Oct 2006).

(Received 8 Sep 2006, accepted 8 Oct 2006) ❑