

The preparedness of hospital Health Information Services for system failures due to internal disasters¹

Cheens Lee, Kerin M Robinson, Kate Wendt and Dianne Williamson

Abstract

The unimpeded functioning of hospital Health Information Services (HIS) is essential for patient care, clinical governance, organisational performance measurement, funding and research. In an investigation of hospital Health Information Services' preparedness for internal disasters, all hospitals in the state of Victoria with the following characteristics were surveyed: they have a Health Information Service/Department; there is a Manager of the Health Information Service/Department; and their inpatient capacity is greater than 80 beds. Fifty percent of the respondents have experienced an internal disaster within the past decade, the majority affecting the Health Information Service. The most commonly occurring internal disasters were computer system failure and floods. Two-thirds of the hospitals have internal disaster plans; the most frequently occurring scenarios provided for are computer system failure, power failure and fire. More large hospitals have established back-up systems than medium- and small-size hospitals. Fifty-three percent of hospitals have a recovery plan for internal disasters. Hospitals typically self-rate as having a 'medium' level of internal disaster preparedness. Overall, large hospitals are better prepared for internal disasters than medium and small hospitals, and preparation for disruption of computer systems and medical record services is relatively high on their agendas.

Keywords (MeSH):

Medical Records; Medical Record Systems, Computerised; Hospital Administration and Organisation; Disaster Planning; Quality of Healthcare

Hospital Health Information Services undertake a critical role in the supply, storage and retrieval of patient health information. Patient health information which is accurate, comprehensive, current and readily available is vital for the administration of quality patient care and treatment by clinicians and nurses, and for clinical governance, organisational performance monitoring, funding and research. Health Information Services primarily develop, implement and manage the systems, technologies and other resources for the compilation, maintenance, storage and retrieval of medical records for use within the hospital; they are also responsible for analysis of the data, the specialised classification of diagnoses and procedures for clinical research, diagnosis-

related grouping for financial reimbursement, and reporting of health information to state health departments and statutory bodies. Unexpected disasters that interrupt these vital services have the potential to be highly disruptive to the hospital and its patients and staff.

Background

What is a disaster?

Imagine this scenario: it is 3.00 am and an electrical fire engulfs a plant room in the basement of a large, metropolitan specialist hospital. It fills wards with smoke, forcing a full-scale evacuation of patients, including newborn babies, and staff.

¹ This research was undertaken when all authors were part of the Department of Health Information Management, School of Public Health, Faculty of Health Sciences, La Trobe University, Australia.

On Wednesday 3 December 2003, for the patients and staff of Melbourne's Mercy Hospital for Women this was not an imaginary scenario (Turner 2005). Luckily, there were no injuries sustained; however the fire caused major disruption to hospital services and the temporary closure of some wards. This exemplifies an internal disaster that can severely disrupt the normal business functions of a hospital.

A disaster can be described as an occurrence that causes serious disruption or disables necessary business functions (Corrigan 1995). Disasters can strike without warning; when they occur, organisations need to have contingency plans in place, initially to restore business functions and subsequently to recover resultant losses.

The literature

There are several theoretical contexts for this study, including clinical governance and risk management, the latter being defined as 'those investment decisions taken by an organisation in anticipation of, or as a consequence to, foreseen losses' (Doherty 1985: 86). Risk carries an associated sense of hazards, dangers and volatility in unexpected outcomes, as well as a long-standing connotation with insurance against financial and other unpreventable but potential losses (Power 2004; Doherty 1985; Sadgrove 2005).

Contingency plans are defined actions that are to be executed when an unplanned-for situation occurs (Steiner 1979). Their primary purpose is to optimise managers' ability to deal with unexpected events or conditions. They constitute a proactive approach to risk management of change and uncertainty, and enable more rational responses in the event of disaster (Hussey 1982; Steiner 1979). Within the context of an information technology environment, it is possible to differentiate between 'contingency plans' which relate to a planned event, and 'business continuity plans' which relate to services and assets that are already operational (Rittinghouse & Ransome 2005). These terms tend to be used interchangeably; another frequently-used descriptor is 'disaster planning' (Johns 2002).

Business continuity or contingency plans involve several steps ranging from preparation for and prevention of a disaster through to establish-

ment of priorities, developing the disaster plan, and planning and preparing for disaster recovery (Frost 1994). Following their study on the use of disaster plans by United Kingdom libraries and archives, Muir and Shenton (2002) concluded that a disaster plan also serves as an important policy and training document. Ideally, the disaster contingency plan identifies all critical business support services and dependencies, is up-to-date and, most importantly, is simple and easy to use and capable of keeping the organisation operational during and after the disaster (Frost 1994; Wainwright 2007). This is particularly important for healthcare facilities because rapid access to accessible and usable patient data is essential (Wainwright 2007).

Hospitals are highly reliant upon information technology to support their Health Information Service and related business functions. Reliable financial, clinical and administrative systems, for example the Patient Master Index (PMI), are as vital for efficient work-flows as planning for technology failures and disruptions. Most contemporary health information technology initiatives (e.g. the HealthSMART program, a whole-of-health information and communication strategy of the Victorian Department of Human Services) have as one of their aims the improvement of patient care by reducing the administrative burden placed on health professionals through the use of standardised information systems; however, a potential risk arises because information technology systems are vulnerable to malicious attacks, technology failures and power failures (Department of Human Services 2009; Tilley 1995). The general awareness of this potential vulnerability was seen prior to the year 2000 when the threat of the 'Y2K' bug triggered a surge in contingency planning for information technology systems (Solomon 2005).

Health Displan Victoria is the state health emergency response plan which centres on a multi-agency medical response to major disasters and the subsequent potential influx of patients to hospitals (Department of Human Services 2006). Beyond '*Displan*', there are emergency plans and recommendations of a general nature such as Standards Australia's AS 4083, 2007 'Planning for emergencies – Health care facilities' (Standards Australia 2007).

The focus of our study, internal disasters that disrupt the normal functions of Health Information Services, has received minimal attention in the literature. There are reported studies on external disasters that disrupt the hospital's routine operations; the foci here tend to be on surge capacity and how Emergency Departments handle an influx of patients following external, man-made or natural disasters, or the longer-term effects of external disasters on the functioning of Health Information Services (Traub, Bradt & Joseph 2007; Dimick 2008). Some research has also been undertaken on planning for external disasters that result in a situation of patient surge affecting Health Information Services; for instance, Buchanan investigated the use of specialised emergency records and contingency plans for disasters (e.g. pre-allocated Unit Record numbers or prepared medical records) and reports good intent but relatively poor activation of these practices by public hospitals (Buchanan 1993). Smith and Macdonald (2006) recommend strategies for disaster preparation by Health Information Services and explain the importance of disaster plans for the continuity of the services. Smith, Morgans, Biggs and Buchanan (2007) also focus on the influx of patients to a hospital in their exploration of the uptake of specialised health information systems during external disasters.

Internal disasters affecting Health Information Services

Publicly documented internal-to-the-hospital disasters that affect Health Information Services are few in number. Two disasters reported in the Australian health information management literature have involved flooding. Sands describes the experience of dealing with the effects of an exceptionally heavy rainfall which resulted in water penetrating the Warringal Private Hospital building and flooding the Health Information Service (Sands 2006). The disaster aftermath included medical record salvage and retrieval, and the prevention of potential confidentiality issues that had to be dealt with by Health Information Managers.

Another internal disaster, of water inundation of the Health Information Service of Melbourne's Royal Children's Hospital, was caused by a

plumbing problem (Cowling, Cassin & Raw 2001). The hospital called a Code Yellow ('Failure of vital internal services'), per the Standards Australia AS4083, 1997 Planning for emergencies – Health care facilities (Standards Australia 1997). The experience of this hospital's Health Information Managers included dealing with the complicated, specialised, and time-consuming tasks of salvage and restoration of medical records, and facilitating continuity of service to clinicians and other stakeholders. The hospital subsequently formed a Disaster Mobilisation Unit in the Health Information Services to respond to future 'Code Yellows' in the department.

The nature of internal disasters and their lower public profile than external disasters means that many go unreported in the public domain.

Aim and objectives

The aim of our research project was to investigate the preparedness of Victorian public and private sector hospitals' Health Information Services for system failures and other problems affecting normal business functioning caused by internal disasters, that is, disasters emanating from within the organisation.

The objectives of the study were:

- to examine the level of preparedness of Victorian public and private hospitals' Health Information Services in the event of system failures
- to investigate whether these Health Information Services have contingency plans for internal disasters.
- to identify which potential risks are planned for in Health Information Services' internal disaster plans
- to inquire into Health Information Services' back-up systems readiness, in the event of system failure following internal disaster
- to determine whether the Health Information Services have recovery plans ready to take effect following an internal disaster
- to identify how Health Information Services rate their own levels of preparedness for internal disasters.

Method

Sample selection

The study population comprised all public and private hospitals in the state and was enumerated using a publicly available data file from the Victorian Department of Human Services. In order to be selected into the study sample, each hospital was required to meet the following three criteria:

- it contained a Health Information Service/department
- it had a bed capacity of greater than 80 admitted beds
- there was a Manager of the Health Information Service/department.

Targeted respondents constituted the Manager of the Health Information Service, or their representative, of each hospital in the sample. The sample size was 69, comprising 42 public sector hospitals and 27 private sector hospitals.

Ethics approval

Approval for the conduct of the study was obtained from La Trobe University's Faculty of Health Sciences Human Ethics Committee.

Study design and procedure

The study data for this quantitative, non-experimental research project were obtained via a self-administered survey instrument. The questionnaire was sent in late November 2007, by surface mail, to each of the qualifying hospitals with an accompanying, explanatory letter and a pre-paid, addressed envelope to facilitate return of the completed survey. Numbering of the questionnaire preserved respondent anonymity for results reporting but enabled telephone follow-up of non-respondents after two weeks.

The survey instrument²

The self-administered questionnaire included 26 items: 13 closed, constrained-choice questions; 11 further closed-choice questions with provision for the respondent to provide numerical details or a brief explanation; and two open questions inviting a short, narrative response. Part 1 of the questionnaire (eight questions) was designed

to elicit details of the respondent facility, including experience of internal disasters in the organisation generally, and affecting the Health Information Service specifically. Part 2 comprised nine questions designed to elicit information about the respondent hospital's disaster planning and plans. Part 3 comprised three questions about the hospital's disaster planning team, and Part 4 (six questions) inquired of the hospital's disaster recovery planning.

The questionnaire was amended prior to use to reflect the outcomes of a pilot trial.

Data analysis

The responses to the closed items were coded. For the purposes of analysis, the respondent hospitals were classified into 'small' (fewer than 150 beds), 'medium' (between 150 and 299 beds), and 'large' (300 or more beds). Data were entered into Microsoft Access for storage and query. The results were migrated to Microsoft Excel to facilitate presentation.

Results

Response rate and study sample

Thirty-eight (55.1%) of the Health Information Services responded, comprising 22 from public sector hospitals and 16 from private sector hospitals. There was a higher response rate within the private hospital sub-group (59% of the private hospitals surveyed) compared with a response rate of 52% from the public sector hospitals.

Table 1 shows the breakdown of respondent hospitals according to size.

All hospital respondents (Managers of the Health Information Service) except one had a tertiary or equivalent level qualification in Health Information Management or Medical Record Administration.

Internal disasters in the last decade

Fifty percent of the hospitals reported that their organisation or Health Information Service had experienced an internal disaster within the previous 10 years. (We note that where the respondent Manager of the Health Information Service had not worked in their hospital for 10 years it was assumed they would have easily elicited this information from longer-serving

² The survey instrument is available upon request.

Table 1: Response rate according to geographical location and hospital size

HOSPITAL SIZE	METROPOLITAN		RURAL		TOTAL
	PUBLIC	PRIVATE	PUBLIC	PRIVATE	
Small	2	11	2	1	16
Medium	4	3	4	0	11
Large	9	1	1	0	11
Total	15	15	7	1	38

colleagues or staff members.) Nine (56%) of the medium-size hospital respondents and four (36%) of the small hospitals had internal disasters in the past decade. Overall, 50% of all respondent hospitals had experienced an internal disaster in that period.

A total of 26 internal disasters were reported by 19 of the respondent hospitals, with some having experienced more than one internal disaster during the past decade. The majority were computer system failures ($n = 10$), followed by floods ($n = 7$). Four hospitals experienced power failure sufficiently severe to constitute an internal disaster and a total of five reported fire, storm and staff industrial action that created or constituted a threat to their operations. Figure 1 shows the types of internal disasters experienced by respondents.

Sixteen (84%) of the 19 hospitals that experienced one or more internal disasters in the past decade reported that there had been an effect on the operations of their Health Information Service. Some of the respondents' comments were:

- "Data on PMI for one day was lost and had to be re-entered e.g. coding etc. service provision was reduced."
- "Records needed to be freeze-dried at significant expense. Approx 3000 records were therefore unavailable for 6 weeks."

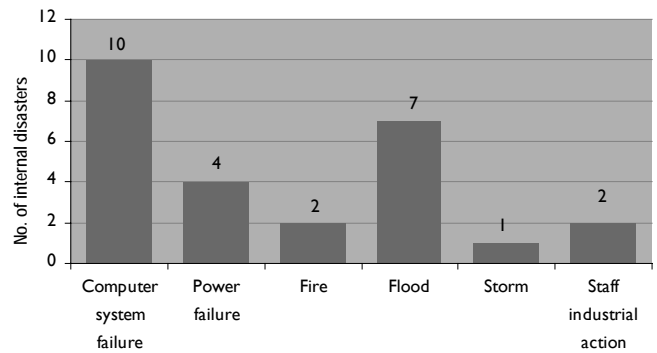


Figure 1: Types of internal disasters experienced in the past decade

- "No access to hospital PMI, back up PMI also down. HIS staff not able to look up record locations or track records out. Manual tracking registers had to be used."

Disaster plans and planning

Some of the respondent Health Information Services have contingency plans for internal disasters or external disasters only; see Table 2. Twenty-four (63%) of the hospitals have contingency plans for both internal and external disasters.

In the case of 30 (78.9%) of the hospitals that have an internal disaster plan, this is overseen or managed by the Manager of the Health Information Service (Chief Health Information

Table 2: Disaster contingency plans in Health Information Services, according to hospital size

HOSPITAL SIZE	INTERNAL DISASTER		EXTERNAL DISASTER		INTERNAL & EXTERNAL		DID NOT ANSWER	TOTAL
	PLAN ONLY		PLAN ONLY		DISASTER PLANS			
	#	%	#	%	#	%	#	%
Small	3	19	0	0	8	50	5	16
Medium	1	9	2	18	7	64	1	11
Large	2	18	0	0	9	82	0	11
Total	6	16	2	6	24	63	6	38

Manager). There are some indications that senior management of the hospitals are also involved with the internal, department-level disaster plans including for the Health Information Services; five (16.7%) of the respondents with internal disaster plans indicated that their Chief Executive Officer and/or the hospital's senior management team have some responsibility for internal disaster plans of the Health Information Service.

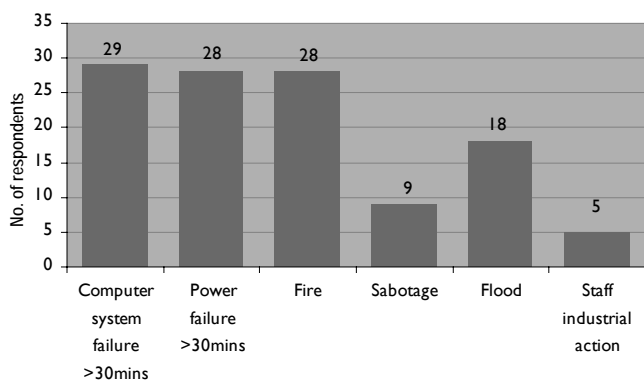


Figure 2: Types of scenarios included in the internal disaster plan(s)

Figure 2 shows that provisions for fire, and computer system and power failures, feature significantly in internal disaster plans.

The survey instrument also invited respondents to report risk scenarios other than the 'major' contingencies that are provided for in their internal disaster plans; the predominant responses are summarised in Figure 2. Additional scenarios planned for are:

- evacuation
- bomb threat
- medical emergency
- security breach
- chemical spill
- lift stuck with staff in it
- water supply disruption
- gas failure
- hazardous material leak
- pager system failure
- sewer blockages
- storm damage
- equipment failure
- clinical risk
- infection risk
- financial risk.

The Health Information Service disaster contingency plans are located in various places.

Respondents were invited to list more than one location, to reflect the reality of their situations. The reported locations include the hospital intranet ($n = 11$ hospitals), departmental folders ($n = 10$), a folder in the Health Information Service Manager's office ($n = 8$), procedure manuals ($n = 7$) and noticeboards ($n = 6$).

Only 21 (55%) of the respondent hospitals have an organisation- or network-wide disaster planning committee. Proportionately more medium and large hospitals report having such a committee (72.7% and 63.3%, respectively), than do small hospitals (37.5%).

The Managers of the Health Information Service in 11 (29%) of the respondent hospitals report being involved with the organisation- or network-wide disaster planning committee.

Resource allocation to disaster planning

Resource allocation by Health Information Services to disaster planning ranges from five (46%) of the large hospitals, to two (9%) of the medium hospitals, to none of the small hospitals.

Respondents who indicated in the affirmative were invited to state what type of resources were allocated by their department. They responded as follows:

- 'equipment backup'
- 'staff, procedures/equipment (disaster records if required)'
- 'budget'
- 'staff'
- 'back up PMI PC'
- 'fire training'.

Back-up systems

There is a distinctive pattern reflected in the hospital Health Information Services that have a back-up system in place in anticipation of an internal disaster. While nine (82%) of the large hospitals report having a back-up system, this is the case for eight (73%) of medium hospitals and 10 (63%) of the small hospital respondents.

The respondents who answered in the affirmative were invited to indicate the type of back-up systems they have established for internal disasters. The answers were varied and we have therefore grouped the responses. Figure 3 shows the top four types of back-up systems listed by

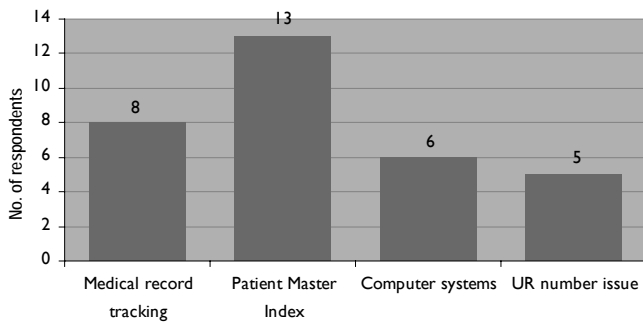


Figure 3: Categories of back-up systems in place for an internal disaster

respondents; some respondents listed more than one type of back-up system.

Disaster planning teams

None of the small hospitals has a planning team for internal disasters. One of the medium hospitals and two of the large hospitals reported having an internal disaster planning team.

Disaster recovery

The larger the hospital, the greater the likelihood of the existence of a recovery plan ready to take effect following an internal disaster: six (38%) of the respondent small hospitals, six (55%) of the medium hospitals, and eight (73%) of large hospitals have a recovery plan. Eighteen (47%) of the respondent Health Information Services have no recovery plan in place.

The disaster recovery plans were reported as being located on the hospital intranet ($n = 8$ hospitals), in a folder in the Health Information Service ($n = 8$), in procedure manuals ($n = 3$), in a folder in the Manager's office ($n = 3$) and on noticeboards ($n = 2$). Hospitals were invited to nominate more than one location, as applicable to their situation.

Preparedness for internal disasters

The hospitals were asked to select the most important factor to consider when preparing for internal disasters. All respondents answered this question, with three (7.9%) hospitals giving invalid answers by selecting more than one option. 'Maintaining normal business function' and 'maintaining patient privacy' were the two most frequently selected factors, with equal responses ($n = 13$; 37.1%); these were followed by 'minimising physical damage to the

HIS infrastructure'. One medium-size hospital selected the option of 'other' and elaborated with the comment: 'ensuring safety of all staff and patients'.

Six respondents indicated a high level of preparedness for internal disasters, while 18 hospitals (47.4%) rated their level of preparedness as 'medium', making it the most frequently chosen level. Ten hospitals stated that they have a low level of preparedness, and six indicated a nil level of preparedness. Similar levels of preparedness were reported for external disasters.

Respondents were invited to provide relevant additional comments and seven (18.4%) chose to comment. A selection of their comments follows:

- 'Kit of 100 disaster records located in the emergency department for external emergencies'
- '...senior management do discuss disaster planning in operations meetings and ensure manuals and procedures are updated and relevant. All staff complete fire safety and aggression management training.'
- 'Contingency planning for other than the "predictable" failures (system downtime, fire/evacuation) has not been considered previously here (eg. Sabotage)'
- 'The term 'disaster' is a very broad category. We have extensive fire preparation organisation wide. For power failure we have data backup procedures and standalone access database.'

The comments show that some scenarios, such as sabotage, have not been considered previously by some respondent hospitals.

Discussion and conclusions

Internal-to-the-hospital disasters can significantly disrupt core functions of Health Information Services including the provision of information to clinicians and other users and the loss of, or irreparable damage to, records and data. Missing medical records or other information may give rise to a situation of clinical risk.

Hospitals rely on computer systems to support health business functions and many clinical functions and the failure of these, and their power supplies, seems more likely to occur than disasters caused by nature; however, the sparse literature in this area reports local hospitals suffering the effects of externally- and internally-generated flooding which can cause permanent

or temporary damage to medical records and threaten the integrity or availability of critical patient information (Sands 2006; Cowling, Cassin & Raw 2001). Approximately two-thirds of Victorian hospital Health Information Services have contingency plans for both internal and external disasters, and a further 16% have plans for internal disasters only. This reflects some recognition of Rittinghouse and Ransome's (2005) concept of business continuity plans in an information technology environment, and the need for rapid access to accessible and usable data (Wainwright 2007). The most commonly prepared-for risks involve computer system and power failures, and fire, although a number of other disruptions are also anticipated. Back-up systems in readiness for internal disasters are more predominant in larger hospitals, the most common being PMI back-up followed by medical record tracking and computer systems. This appears to indicate that Health Information Managers regard preparation for uninterrupted functionality of core systems to be paramount whereas the less predictable potentialities such as equipment failure, bomb threat and failure of or disruption to utilities and related services, have less import. It may be cause for concern that there is lack of uniformity in preparedness, with larger hospitals being generally better prepared than smaller hospitals in terms of internal disaster contingency planning, related resource allocation, and recovery plans.

Limitations of the research

This research is limited to Health Information Services in Victorian hospitals. It may or may not be generalisable to hospitals beyond Victoria, in part because of possible differences between Health Information Service business functions.

Concluding comments

Our study has provided a picture of the preparedness of Victorian hospital Health Information Services for the effects of internal-to-the-hospital disasters. We conclude that there is value in having disaster contingency and recovery plans in place to mitigate potential harm to patients. We hope that our research will raise awareness of the need for preparedness for internal disasters.

References

- Buchanan, W. R. (1993). *Specialised emergency records for disasters used in Victorian public hospitals*. Health Information Management Honours thesis, La Trobe University.
- Corrigan, P. (1995). Defying disaster. *LAN Magazine* 10(8): 89-91.
- Cowling, S., Cassin, K. and Raw, J. (2001). Restoring water-damaged medical records: the great flood of 2001. *Health Information Management Journal* 30(2).
- Department of Human Services (2006). *State health emergency response plan*. Health Displan Victoria. Melbourne, Victorian Department of Human Services. Available at: http://www.dhs.vic.gov.au/emergency/health_displan (accessed 6 April 2009)
- Department of Human Services (2009). *HealthSMART* (online). Melbourne, Victorian Department of Human Services. Available at: <http://www.health.vic.gov.au/healthsmart/> (accessed 6 April 2009).
- Dimick, C. (2008). A long recovery: HIM departments three years after Katrina. *Journal of the American Health Information Management Association (AHIMA)* 79(9): 42-46.
- Doherty, N. A. (1985). *Corporate risk management: a financial exposition*. New York, McGraw-Hill.
- Frost, C. (1994). Effective responses for proactive enterprises: business continuity planning. *Disaster Prevention and Management* 3(1): 7-15.
- Hussey, D. E. (1982). *Corporate planning theory and practice*. Oxford, Pergamon Press.
- Johns, M. L. (2002). *Information management for health professions*. Albany, NY, Delmar Thomson Learning.
- Muir, A. and Shenton, S. (2002) If the worst happens: the use and effectiveness of disaster plans in libraries and archives. *Library Management* 23(3): 115-123.
- Power, M. (2004). *The risk management of everything: rethinking the politics of uncertainty*. London, Demos.
- Rittinghouse, J. W. and Ransome, J.F. (2005). *Business continuity and disaster recovery for infosec managers*. Amsterdam, Elsevier.
- Sadgrove, K. (2005). *The complete guide to business risk management*. Aldershot, Hampshire, Gower Publishing Limited.
- Sands, J. (2006). Warringal Private Hospital Health Information Service flood disaster recovery: Wednesday 3 December 2003. *Health Information Management Journal* 35(2): 42-44.

- Smith, E., Morgans, A., Biggs, J. and Buchanan, W. R. (2007). Managing health information during disasters: a survey of current specialised health information systems in Victorian hospitals. *Health Information Management Journal* 36(1): 23-29.
- Smith, E. and MacDonald, R. (2006). Managing health information during disasters. *Health Information Management Journal* 35(2): 8-13.
- Solomon, H. (2005). Y2K: the disaster that wasn't. *Computing Canada* 31(13).
- Standards Australia (2007). *AS 4083, 2007 Planning for emergencies – health care facilities*. Sydney, Standards Australia Ltd.
- Standards Australia (1997). *Planning for emergencies - health care facilities*. Sydney, Standards Australia Ltd.
- Steiner, G. A. (1979). *Strategic planning: what every manager must know*. New York, Free Press.
- Tilley, K. (1995). Work area recovery planning: the key to corporate survival. *Facilities* 13(9/10): 49-53.
- Traub, M., Bradt, D.A. and Joseph, A. (2007). The surge capacity for people in emergencies (SCOPE) study in Australasian hospitals. *Medical Journal of Australia* 186(8): 394-398.
- Turner, A. (2005). Merciful solution to hospital fire crisis. *The Age* 15 February: 7.
- Wainwright, V. L. (2007). Business continuity by design: don't let a disaster impair your facility's performance (Business Continuity Management). *Health Management Technology* 28(3): 20-21.

Cheens Lee *BHlthInfoManagt(Hons)*
Solution Consultant
iSOFT
email: cheens.lee@isofthealth.com

Corresponding author:

Kerin M Robinson *BHA, BAppSc(MRA), MHP, CHIM*
Head, Health Information Management Program
School of Public Health, Division of Health Studies
Faculty of Health Sciences
La Trobe University
Bundoora VIC 3086
AUSTRALIA
Tel: +61 3 9479 5722
email: K.Robinson@latrobe.edu.au

Kate Wendt *BMedRecAdmin, GradDipHlthServMgt*
Lecturer, Health Information Management Program
School of Public Health, Division of Health Studies
Faculty of Health Sciences
La Trobe University
Bundoora VIC 3086
AUSTRALIA

Dianne Williamson *BAppSc(MRA), GradDipErg*
Senior Lecturer, Health Information Management Program
School of Public Health, Division of Health Studies
Faculty of Health Sciences
La Trobe University
Bundoora VIC 3086
AUSTRALIA ■

This research was undertaken when all authors were part of the Department of Health Information Management, School of Public Health, Faculty of Health Sciences, La Trobe University, Australia.

Could your Professional Standing survive a loss of patient information?



What about...

Computer Failure?

Data Loss may not be readily retrievable as tape and disc backups tend to have a 30% + failure rate.

Virus?

51% of spyware comes from accessing legitimate sites.

Theft?

A laptop is stolen in Australia every 10 minutes.

Fire or Flood?

Disasters destroy not only current information but also backups made onsite.

Your information is vital to patient welfare.

Keep it healthy with Automated Secure Online Backups.



Phone (02) 9317 0900
Email info@file.com.au
Web filevault.com.au



FILE Pty Ltd.