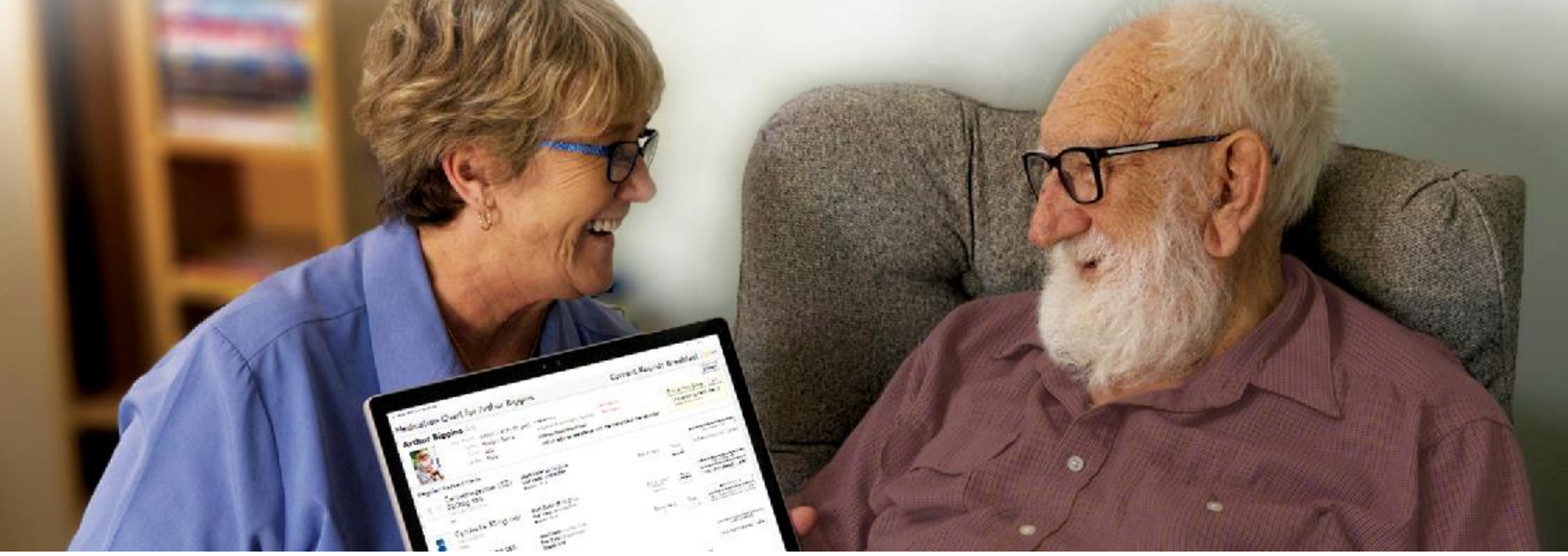
AutumnCare



White Paper

AutumnCare Connect
AutumnCare Medicate
Elderly Care
Healthcare
Disaster Recovery
Business Continuity
Management

Business Continuity and Disaster Recovery for Elderly Care

Maintaining clinical operability in the event of disasters can be realised through AutumnCare's electronic care management system.

Clinical systems require uninterrupted access to information together with the ability to continue to record data at all times. Anything less puts people at risk and compromises the safety and quality of care.

This paper will help the reader in conducting an assessment of the broad amount of Information Technology (IT) risk that it is willing to accept in pursuit of its objectives (risk appetite) and how they should plan for disaster recovery and business continuity. As IT becomes critical to aged care operations, disruptions to normal business must be planned for and managed.

Challenge	Ensuring continuous clinical operations in the event of a major disaster affecting power, access to database servers, telecommunications and inaccessibility of the aged care facilities.
Solution	AutumnCare Connect's Enterprise clinical management system, providing access to a range of clinical information with its in-built Business Continuity and Disaster Recovery functionality.
Impact	Eliminates the need to activate disaster recovery plans for clinical operations. Full access to clinical information – notes, care plans and assessments is assured. Data can continue to be created and is automatically synchronised on restoration of connectivity.

AutumnCare

AutumnCare is a software company operating in Australia and the United Kingdom and expanding into other markets. AutumnCare's key business is the engineering of robust, enterprise grade clinical operational systems.

AutumnCare ensures organisations can continue to function and deliver care in the event of disaster, ensuring safety and quality of care is provided to their Residents.

CIO Questions:

- Is your organisation able to work during a disaster?
- Do you require paper or other manual back-up systems?
- How long will it take to restore your servers?
- Do you have a platform replacement strategy?
- How long will it take to restore from catastrophic network failure?
- Do you have emergency communication facilities in place?
- Does your team have the skills to recover from multiple scenarios?
- Are your plans tested on a regular basis?

.

Business Continuity and Disaster Recovery encompass many potential scenarios that could affect an organisation’s operations. A key element for continuity is Information Technology (IT). That is, in the event of a disaster, such as the main data centre being destroyed, information and data should be available to support the fundamental continuing operations of the organisation.

Organisations and CIOs need to be prepared for disaster, and there is always a lot of talk in the industry around making effective use of technology for Disaster Recovery (DR) solutions. However, for all of the talk and the technology available to organisations they do not tend to be fully prepared for disaster.

What they are typically prepared for are a set of scenarios that may not cater for every situation. When a disaster occurs the chaotic situation that ensues makes the execution of plans difficult.

The AutumnCare solution is unique in that it allows the organisation to remain operational throughout the disaster while restoration solutions are being implemented. It gives the organisation time to work though optimal recovery strategies.

Typical IT risks and mitigation strategies are all covered by AutumnCare. Including operational risks such as server failure, deployment risks such as using appropriate software architectures etc. with potential mitigation strategies being organisationally implemented.

Business continuity planning should not be an event, but an ongoing process. Therefore, an overall governance framework for the management of information and systems needs to be in place.

Disaster Recovery Overview

Since the start of business computing in the 1960s, users and managers of Information Technology (IT) began to recognize that their rapidly growing centralised computing centres were becoming Single Points of Failure (SPOF). Businesses realised that whilst there were great advantages to centralised operations and data, any interruption had a very significant impact on the critical operational functions. The viability of the business itself could even be threatened. Computing hardware, supporting network infrastructures, and software platforms are full of SPOFs that need particular strategies to reduce the likelihood of and risk of failure impact.

The general strategy to avoid single points of failure has been to duplicate the computing resources used. Sophisticated hardware and devices have been employed to reduce the possibility of a single point of failure affecting the business

operations. RAID disk setups, redundant servers, duplicate networks, duplicate communications devices, back-up power supplies, non-stop servers etc. These solutions are expensive to purchase, manage and maintain and still do not eliminate the issue of single points of failure affecting business operations. For instance, if a main optical fibre feeding the area where the central server is located is cut then all parts of the business relying on that server will be without computing ability.

AutumnCare recommends using best practice to ensure the risks of server failure are minimised.

AutumnCare uses a unique design philosophy that has been adopted to eliminate single points of failure affecting the end users.

AutumnCare has adopted the following architectures:

1. **Service Oriented Architecture**
   This is architectural best practice that delineates the database from business logic; enables scaling and a high level of security and provides for interoperability.
2. **Occasionally Connected Computing**
   This model provides the ability to work off-line and has been designed to be an integral part of all AutumnCare products.
   It is coupled with a unique transaction engine and supporting algorithms. It provides for continuous operation during any outage.
   This architectural construct also allows for:
   a. Restoration of data from client machines
   b. Flexible maintenance windows and
   c. Simplifies upgrade processes.

AutumnCare's **unique architecture:**

- Allows the end users to keep working and inputting data thereby eliminating the need for costly manual back-up systems.
- Facilitates rapid recovery in case of server or server access failure and data recovery if data is lost.
- Contains constructs that allow switching to standby sites.

AutumnCare also supports database replication so a "belts and braces" approach can be implemented in data centres.

There are numerous examples where AutumnCare has ensured continuous clinical operation.

1. The catastrophic 2015 NSW floods saw many facilities cut off from power and telecommunications. AutumnCare ensured continuous clinical operation and no adverse outcomes.
2. Western Australian 2016 bushfires saw facilities evacuated. AutumnCare ensured continuous operation, even during bus transfers, and the ability to reconnect at the emergency sites.
3. An AutumnCare client experienced catastrophic server failure and discovered their back-ups had been failing for the previous 5 days. The AutumnCare end users kept working and entering data while the new server was established with the last viable back-up and all the missing data was easily recovered in a few hours.

The above highlights the **resilience** of AutumnCare and the need for processes and checks to ensure your information systems are protected.

Contact AutumnCare for more information on any of the concepts discussed within this white paper.

info@autumn.care

1800 422 472 | Int +61 08 9472 0444

Visit our website for more on the benefits of a robust, enterprise grade clinical operational system.

www.autumn.care

AutumnCare