# Case study: Ransomware attack

**Scenario: A medium-sized practice experienced a ransomware attack that encrypted patient records and disabled critical systems. The attack was identified when staff could not access patient files.**

#### Immediate Response:

* At 9am on a Monday morning in a busy practice, the PMS was no longer accessible. Following a slight panic the receptionist notified the practice manager. Impact is – no patient records are accessible.

#### Incident Response activated

* The practice manager and staff activated the Business Continuity Plan (BCP) so that they could carry on with their daily business. IT investigated the incident following a call from the practice manager. IT and the practice manager maintained close contact.

#### Assessment and Documentation

* IT established that data was involved and had been accessed. They confirmed it was a cyber attack involving patient personal information. The privacy officer, the practice manager and IT conducted a rapid risk assessment. It was indicated that sensitive patient information was compromised, including treatment histories. Approximately 3 hours following the attack a ransom note was detected.

#### Immediate Notification

* Following the rapid risk assessment and based on the guidance provided by the OPC a decision was made to notify the OPC and the Police of the incident – due to the criminal nature of the attack.
* Patients on-site and due to have an appointment were informed about technical issues impacting services.
* Additional staff were secured to help manage some of the manual workarounds that were required.

#### Evaluation of Risks and Impacts

* IT, the practice manager and the privacy officer continued to work together closely to understand the incident.
* A detailed privacy assessment was started which highlighted a high risk to patient confidentiality. Simultaneously the BCP was activated to maintain basic healthcare services. This meant:
* Patients at the practice were alerted that there was an issue with the IT systems, and access to their histories were restricted. Patients onsite
* were seen, and their notes were hand documented. Patients who were yet to arrive were contacted and requested to defer their appointments unless urgent.
* A sister practice was contacted to request availability for appointments.
* Some staff were requested to go home in-case to preserve energy.
* Meanwhile IT worked hard to understand the timeframe to back up systems and secure the system from any unauthorised access.
* Constant re-evaluation was needed to understand the impacts and the timeframe to restoration.

#### Notification of Impacted Individuals

* In parallel a notification strategy was developed in-line with the assessment of the information, and a decision was made to contact impacted patients through secure emails and letters. Considerations included standing up a phone line to support impacted information around the content of the information contained in the breach and to provide assistance on how to safeguard their security.

#### Recovery and Mitigation

Once the breach was contained and systems were secured and backed up, the team was able to focus on working through the lessons learned of the incident, which included:

* Ensuring that the staff were able to have some well-deserved time off.
* Making sure that BCP activities were documented and any additions to patient records were transcribed back into the system – ensure have enough staff.
* Security measures were strengthened, including enhanced encryption and employee training on cybersecurity.
* Insurance plans were updated with vendors to facilitate response.
* Full review of the incident was undertaken to further learn, improve and document.

#### Ongoing Management and Review

* The incident’s handling was reviewed with all business stakeholders prompting discussion and ensuring compliance with regulatory requirements.

#### Lessons learned:

* The practice were astounded at quite how fast paced the response needed to be. The pressure on staff was enormous. The activities that needed to be completed in parallel were intense and required a multi-disciplinary team. The practice manager decided to engage in cyber security training measures, incident response using CIMS and privacy training for the staff.