# Case study: DDoS/Data exfiltration

**Scenario: A medium-sized Practice experienced a DDoS attack – this was a smokescreen for data exfiltration attack.**

#### Immediate Response:

* On a Monday morning, the online patient portal and the practice’s internal network experienced severe slowdowns and intermittent outages. Patients were unable to access their records, book appointments, or communicate with the practice via the portal. The IT team was alerted, and initial investigations revealed an ongoing Distributed Denial of Service (DDoS) attack targeting the practice’s servers.

#### Incident Response Activated:

* The practice manager, IT team, and privacy officer immediately activated the BCP. IT began to mitigate the DDoS attack by redirecting traffic and increasing server capacity. The privacy officer documented the incident while staff switched to manual processes to continue patient care.

#### Assessment and Documentation:

* As the DDoS attack was being mitigated, the IT team noticed unusual activity on the internal network. Several unauthorised login attempts were detected, which indicated that the DDoS attack might be a smokescreen for a more sophisticated cyber attack. A rapid risk assessment was conducted with the practice manager and the privacy officer, and the IT team immediately escalated the findings as acute, recognising that sensitive patient data could be at risk.

#### Secondary Attack Detected:

* Further investigation confirmed that during the height of the DDoS attack, the hackers had successfully infiltrated the system using the disruption as a distraction. They had accessed patient records and exfiltrated sensitive data, including personal identification details and medical information. The attackers had exploited vulnerabilities in the network while the IT team was focused on combating the DDoS attack.

#### Immediate Notification:

* OPC and Police were notified of the dual nature of the attack. The practice also informed their cybersecurity insurance provider. Patients were not immediately informed as the extent and severity of the data breach was still being assessed, but they were notified of potential delays in service due to ongoing technical issues.

#### Evaluation of Risks and Impacts:

* The IT team, along with an external cybersecurity firm, began a thorough assessment of the breach. It was determined that the attackers had accessed a significant amount of sensitive patient information. The privacy officer conducted a detailed privacy assessment, which indicated a high risk to patient confidentiality.