CAPSTONE
SYSTEM

PRIVACY POLICY

Capstone System treats all information with the utmost respect and confidentiality. Our commitment to privacy involves the following:

Secure Data Location

Capstone System stores all data in Microsoft Azure datacentres within Australia. Microsoft's security protocols include:

Assume breach

The guiding principle of Microsoft's security strategy is to "assume breach." The Microsoft global incident response team works around the clock to mitigate the effects of any attack against our cloud services. And security is built into Microsoft business products and cloud services from the ground up, starting with the Security Development Lifecycle, a mandatory development process that embeds security requirements into every phase of the development process.

Auditing and logging

Protect data by maintaining visibility and responding quickly to timely security alerts.

Dedicated cybersecurity teams

Microsoft has invested in multiple cybersecurity teams and related facilities to address threats to our customers and our technology ecosystem.

Fighting cybercrime

The Microsoft Digital Crimes Unit (DCU) mission is to provide a safer digital experience for individuals and organizations worldwide by helping to protect vulnerable populations, fight malware, and reduce digital risk.

Protecting your enterprise

The Microsoft Enterprise Cybersecurity Group is a team of world-class architects, consultants, and engineers that works with organizations to help move them to the cloud more securely, modernize their IT platforms, and avoid and mitigate breaches.
Defending against cyberthreats

The Microsoft Cyber Defense Operations Center is a state-of-the-art facility that brings together security response experts from across the company to help protect, detect, and respond to cyberthreats in real-time—all day, every day.

Setting security policy for a connected world
The Microsoft Cybersecurity Policy Team partners with governments and policymakers around the world, blending technical acumen with legal and policy expertise. By identifying strategic issues, assessing the impacts of policies and regulations, leading by example, and driving groundbreaking research, the Cybersecurity Policy team helps promote a more secure online environment.

Platform Security

Microsoft believes that security doesn't end in the public cloud. Security needs to be engineered into a system end to end, from the public cloud all the way to the desktop. From the very beginning, Microsoft architected their cloud services platform with multiple levels of security that are virtually and physically isolated. Your data is protected by hardened operating systems and backed by a defense-in-depth strategy that helps protect our cloud services.

In addition, Microsoft have continuous, proactive, and reactive threat monitoring and analytics. Microsoft also encrypt customer data at rest and in transit, and encrypt customer data that passes between our datacenters. Every datacenter is constructed, managed, and monitored to protect data from unauthorized access. Microsoft also do not engineer backdoors into our services.

Network Security

Microsoft provide secure communications between your infrastructure and our cloud services and block unauthorized traffic. Specific platform security features include:
SQL Always Encrypted gives you the tools to encrypt sensitive data, such as credit card numbers and national identification numbers, and stored it in Azure SQL Database or SQL Server databases. SQL Always Encrypted creates data separation between those who own the data (authorized users) and those who manage the data (cloud database operators or administrators).

Multi-factor authentication and Credential Guard technology is built into Windows 10 to help you go beyond passwords and move to more secure forms of authentication, such as PINs and biometrics, using the security capabilities already built into your Windows devices. These technologies help organizations defend against identity compromise and pass-the-hash attacks.

Secure Identity

Microsoft uses stringent identity management and access controls to limit data and systems access to those with a genuine business need (least-privileged). Account password controls enforce password complexity rules and require periodic rotation. Microsoft implement system design and policies to prevent personnel who have authorized access to customer data from using it for purposes beyond those identified for their roles. Security policies set the standards and define procedures for data protection.

Microsoft has invested in systems and controls that automate most Office 365 operations while intentionally limiting Microsoft personnel access to customer content. Humans govern the service, but software operates it. This enables Microsoft to manage Office 365 at scale, and to manage the risks of internal threats to customer content (such as malicious actor or the spear-phishing of a Microsoft engineer).

As an example: By default, Microsoft engineers have no standing administrative privileges and no standing access to customer content in Office 365. A Microsoft engineer may have restricted (and audited) secured access to a customer's content for a limited amount of time, only when necessary for service operations and only when approved by a member of senior management at Microsoft (and, for customers who are licensed for the Customer Lockbox feature, the customer).

Microsoft subcontractors are held to the same security standards as full-time employees. Subcontractors who work in facilities or on equipment controlled by Microsoft must follow our data protection standards, and all other subcontractors must follow data protection standards that are equivalent to our own. Microsoft subcontractor agreements are designed to ensure the safeguarding of customer information, and subcontractors' work is regularly monitored.

Secure Infrastructure

Operational Security Assurance (OSA) makes Microsoft business cloud services more resilient to attack by decreasing the amount of time needed to prevent, detect, and respond to real and potential Internet-based security threats. It ensures that operational activities follow rigorous security guidelines and validates that these guidelines are followed. When issues arise, a feedback loop helps ensure that future revisions of OSA support mitigations that address them.

An "assume breach" strategy enables Microsoft to harden its business cloud services and stay ahead of emerging threats. In this approach, the design, engineering, and operations teams assume that attackers have already exploited vulnerabilities or gained privileged access. A dedicated "red team" of security experts simulates real-world attacks at the network, platform, and application layers, challenging the ability of Microsoft Azure and Microsoft Office 365 to detect, protect against, and recover from security breaches.

Threat Management

Threat management includes protection from both malicious software and attacks against systems and networks. Microsoft products and services have built-in protection features to help defend your data against malware and other types of threats.
Microsoft cloud services help you protect against malware threats in multiple ways. Microsoft Antimalware is built for the cloud, and additional antimalware protections are provided in specific services. Denial-of-service (DoS) attacks can deny access to important resources and result in lost productivity, so Microsoft builds its services to defend against such attacks. Windows server and client operating systems include multiple technologies for protecting against these threats at the local level.

Australian Government Certification

Importantly, Microsoft Azure holds IRAP certification from the Australian Government and "will not Customer Data or derive information from it for any advertising or similar commercial purposes."

Please find the full version of the Microsoft Online Services Privacy Statement here:
https://www.microsoft.com/en-us/privacystatement/OnlineServices/

Additional information can be found at the Microsoft Trust Centre
https://www.microsoft.com/en-us/TrustCenter/default.aspx

Capstone System has also implemented strategic privacy and security protocols in the governance of information. These include:

SSL encryption

Access to Capstone System is via Secure Socket Layer 256 bit encryption. SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral. SSL is an industry standard and is used by millions of websites in the protection of their online transactions with their customers.

SSL allows sensitive information such as credit card numbers, medicare numbers, and login credentials to be transmitted securely. Normally, data sent between browsers and web servers is sent in plain text—leaving you vulnerable to eavesdropping. If an attacker is able to intercept all data being sent between a browser and a web server, they can see and use that information.

More specifically, SSL is a security protocol. Protocols describe how algorithms should be used. In this case, the SSL protocol determines variables of the encryption for both the link and the data being transmitted.

SSL secures millions of peoples' data on the Internet every day, especially during online transactions or when transmitting confidential information. Internet users have come to associate their online security with the lock icon that comes with an SSL-secured website or green address bar that comes with an extended validation SSL-secured website. SSL-secured websites also begin with https rather than http.

Two-Step Verification

Two-Step verification is a security feature for Capstone System that’s designed to prevent anyone else from accessing or using your account, even if they know your password.

It requires you to verify your identity using your mobile phone before you can access your account from a new IP address.

Two-step verification helps protect you by making it more difficult for someone else to sign in to your Capstone System account.

Encrypted Patient Data

Specific patient data and user passwords are encrypted at the database level (MySQL) in Capstone System. Encryption is a modern form of cryptography that allows a user to hide information from others. Encryption uses a complex algorithm called a cipher in order to turn normalized data (plaintext) into a series of seemingly random characters (ciphertext) that is unreadable by those without a special key in which to decrypt it. Those that possess the key can decrypt the data in order to view the plaintext again rather than the random character string of ciphertext.

IP Restricted Access

IP Restricted Access is provided as a security and privacy feature. Users can be authorised for to access the system from a single IP address or multiple (dynamic). Under the “dynamic” setting, access from a new IP address requires Two-Step Verification to obtain access to your account.

Staff & Personnel

All Capstone System staff and external contractors are required to sign a detailed confidentiality agreement encompassing the details, procedures, and all sensitive information relating to, but not limited to our patient information. Access to production environments is also limited to senior staff. Where possible, screen-share technology is engaged in the viewing of patient data in production systems to prevent local access by Capstone Staff.