



سياسة حماية البيانات والخصوصية Data Protection and Privacy Policy

ننبض برعايتك
Caring with every
Heartbeat

1.Introduction to Data Privacy Policy

National Medical Care Company, its branches, and its subsidiaries is committed to protecting the privacy and confidentiality of personal data processed during the delivery of healthcare services and the operation of hospital functions. As a healthcare organization, the processes a significant volume of personal data, including sensitive personal data such as medical and health information, employee records, and operational data related to patients, visitors, and service providers.

This Internal Data Protection and Privacy Policy establishes the principles, rules, and responsibilities governing how personal data must be handled within the Hospital. The policy ensures that all personal data is processed in a lawful, fair, transparent, and secure manner in accordance with the Kingdom of Saudi Arabia Personal Data Protection Law (KSA PDPL), its Implementing Regulations, and other applicable regulatory requirements.

The purpose of this policy is to:

- Ensure that personal data is processed lawfully and responsibly across all hospital departments.
- Protect the rights and privacy of individuals whose data is processed by the Hospital.
- Establish clear roles, responsibilities, and procedures for handling personal data.
- Ensure the secure collection, storage, use, sharing, and disposal of personal data.
- Promote a culture of data protection awareness and accountability among all hospital employees and authorized personnel.

All employees, contractors, medical staff, and third parties working with the Hospital must adhere to the requirements outlined in this policy when handling personal data.

1.2 What is Personal Data and Sensitive Data

Under the KSA Personal Data Protection Law (PDPL), personal data refers to any information relating to an identified or identifiable individual. An individual may be identified directly or indirectly through identifiers such as a name, identification number, location data, or other factors related to the individual's identity.

١. مقدمة عن سياسة خصوصية البيانات

تلتزم الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة بحماية خصوصية وسرية البيانات الشخصية التي تتم معالجتها أثناء تقديم خدمات الرعاية الصحية وتشغيل وظائف المستشفى. وبصفتها جهة صحية، تقوم بمعالجة حجم كبير من البيانات الشخصية، بما في ذلك البيانات الشخصية الحساسة مثل المعلومات الطبية والصحية، وسجلات الموظفين، والبيانات التشغيلية المتعلقة بالمرضى والزوار ومقدمي الخدمات.

تحدد هذه السياسة الداخلية لحماية البيانات والخصوصية المبادئ والقواعد والمسؤوليات التي تحكم كيفية التعامل مع البيانات الشخصية داخل المستشفى. وتضمن هذه السياسة أن تتم معالجة جميع البيانات الشخصية بطريقة نظامية وعادلة وشفافة وآمنة، وذلك وفقاً لنظام حماية البيانات الشخصية في المملكة العربية السعودية ولوائح التنفيذ، بالإضافة إلى المتطلبات التنظيمية الأخرى ذات الصلة.

وتهدف هذه السياسة إلى:

- ضمان معالجة البيانات الشخصية بشكل نظامي ومسؤول في جميع أقسام المستشفى .
- حماية حقوق وخصوصية الأفراد الذين تتم معالجة بياناتهم من قبل المستشفى .
- تحديد أدوار ومسؤوليات وإجراءات واضحة للتعامل مع البيانات الشخصية .
- ضمان جمع وتخزين واستخدام ومشاركة وإتلاف البيانات الشخصية بشكل آمن .
- تعزيز ثقافة الوعي بحماية البيانات والمسؤولية لدى جميع موظفي المستشفى والأشخاص المخولين .

يجب على جميع الموظفين والمتعاقدين والكوادر الطبية والأطراف الثالثة المتعاملين مع المستشفى الالتزام بالمتطلبات الواردة في هذه السياسة عند التعامل مع البيانات الشخصية.

١,٢ ما هي البيانات الشخصية والبيانات الحساسة

وفقاً لنظام حماية البيانات الشخصية في المملكة العربية السعودية، تُعرف البيانات الشخصية بأنها أي معلومات تتعلق بفرد مُعرف أو يمكن التعرف عليه. ويمكن تحديد هوية الفرد بشكل مباشر أو غير مباشر من خلال معرفات مثل الاسم أو رقم الهوية أو بيانات الموقع أو أي عوامل أخرى مرتبطة بهويته.

ومن أمثلة البيانات الشخصية التي تتم معالجتها داخل المستشفى:

Examples of personal data processed within the Hospital may include:

- Patient name, contact details, and identification numbers.
- National ID or Iqama number.
- Date of birth, gender, and nationality.
- Contact information such as phone number and address.
- Employee personnel records.
- Visitor registration details.
- System access logs and CCTV recordings.

- اسم المريض وبيانات الاتصال وأرقام التعريف.
- رقم الهوية الوطنية أو رقم الإقامة .
- تاريخ الميلاد والجنس والجنسية.
- معلومات الاتصال مثل رقم الهاتف والعنوان.
- سجلات شؤون الموظفين.
- بيانات تسجيل الزوار.
- سجلات الدخول إلى الأنظمة وتسجيلات كاميرات المراقبة.

In addition to personal data, the National Medical Care Company and its business units also processes Sensitive Personal Data, which requires a higher level of protection under PDPL.

وبالإضافة إلى البيانات الشخصية، تقوم الشركة الوطنية للرعاية الطبية ووحدات أعمالها أيضا بمعالجة البيانات الشخصية الحساسة، والتي تتطلب مستوى أعلى من الحماية وفقاً للنظام.

Sensitive personal data includes, but is not limited to:

وتشمل البيانات الشخصية الحساسة، على سبيل المثال لا الحصر:

- Health and medical information (diagnoses, treatment records, and all kinds of tests results).
- Biometric data used for identification.
- Genetic information.
- Religious or intellectual beliefs.
- Criminal records.
- Racial or ethnic origin.
- Any data indicating parental status or family relationships.

- المعلومات الصحية والطبية (مثل التشخيصات، سجلات العلاج، ونتائج الفحوصات والاختبارات المخبرية بمختلف أنواعها).
- البيانات الحيوية المستخدمة للتعريف.
- المعلومات الجينية.
- المعتقدات الدينية أو الفكرية.
- السجلات الجنائية.
- الأصل العرقي أو الإثني.
- أي بيانات تشير إلى الحالة الأبوية أو العلاقات الأسرية.

Because healthcare operations require the processing of sensitive health information, the Care Hospitals applies enhanced safeguards and strict access controls to ensure such data is processed only when necessary and in compliance with applicable laws.

نظراً لأن العمليات الصحية تتطلب معالجة معلومات صحية حساسة، فإن مستشفيات رعاية تطبيق ضوابط حماية معززة وإجراءات صارمة للتحكم في الوصول، لضمان معالجة هذه البيانات فقط عند الضرورة وبما يتوافق مع الأنظمة المعمول بها.

1.3 Collecting and Processing Personal Data

The Care Hospitals collects and processes personal data to support its core mission of delivering safe and effective healthcare services, managing hospital operations, and complying with regulatory obligations.

Personal data may be collected from various sources, including:

١,٣ جمع ومعالجة البيانات الشخصية

تقوم مستشفيات رعاية بجمع ومعالجة البيانات الشخصية لدعم مهمتها الأساسية في تقديم خدمات رعاية صحية آمنة وفعالة، وإدارة عمليات المستشفى، والامتثال للمتطلبات التنظيمية. وقد يتم جمع البيانات الشخصية من مصادر متعددة، بما في ذلك:

- Patients and their families during registration, diagnosis, treatment, and billing.
- Employees and medical staff during recruitment and employment management.
- Visitors entering hospital facilities.
- Service providers and contractors supporting hospital operations.
- Digital systems and medical devices used in healthcare delivery.

Personal data may be processed for purposes such as:

- Providing medical care and treatment.
- Maintaining patient medical records.
- Managing appointments and hospital admissions.
- Processing insurance and billing transactions.
- Managing employment and workforce administration.
- Ensuring hospital safety and security.
- Complying with legal, regulatory, and reporting requirements

The Hospital ensures that personal data is processed only when a lawful basis exists under PDPL, such as consent, contractual necessity, legal obligation, protection of vital interests, or other lawful grounds permitted by the law.

The Care Hospitals also ensures that individuals are provided with clear privacy notices explaining how their personal data is collected, used, and protected.

1.4 Collecting and Processing Personal Data

National Medical Care Company, its branches, and its subsidiaries integrates privacy and data protection considerations into all systems, processes, and services that involve the processing of personal data.

The principle of Privacy by Design and by Default requires that data protection measures be incorporated into the development and operation of systems and processes from the earliest stages.

- المرضى وأفراد أسرهم أثناء التسجيل والتشخيص والعلاج والفوترة.
- الموظفون والكوادر الطبية خلال مراحل التوظيف وإدارة شؤون العمل.
- الزوار الداخلين إلى مرافق المستشفى.
- مقدمو الخدمات والمتعاقدون الداعمين لعمليات المستشفى.
- الأنظمة الرقمية والأجهزة الطبية المستخدمة في تقديم الرعاية الصحية.

كما قد تتم معالجة البيانات الشخصية لأغراض متعددة، منها:

- تقديم الرعاية الطبية والعلاج.
- حفظ السجلات الطبية للمرضى.
- إدارة المواعيد وإجراءات تنويم المرضى بالمستشفى.
- معالجة مطالبات التأمين والفوترة.
- إدارة الموارد البشرية وشؤون الموظفين.
- ضمان سلامة وأمن المستشفى.
- الامتثال للمتطلبات القانونية والتنظيمية ومتطلبات الإبلاغ.

وتحرص المستشفى على أن تتم معالجة البيانات الشخصية فقط عند توفر أساس نظامي وفقاً للنظام، مثل الحصول على الموافقة، أو الضرورة التعاقدية، أو الالتزام القانوني، أو حماية المصالح الحيوية، أو غيرها من الأسس النظامية المسموح بها. كما تضمن مستشفيات رعاية تزويد الأفراد بإشعارات خصوصية واضحة تشرح كيفية جمع بياناتهم الشخصية واستخدامها وحمايتها.

١,٤ جمع ومعالجة البيانات الشخصية

تقوم الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة بدمج اعتبارات الخصوصية وحماية البيانات في جميع الأنظمة والعمليات والخدمات التي تتضمن معالجة البيانات الشخصية.

ويستلزم مبدأ الخصوصية منذ التصميم وبشكل افتراضي تضمين تدابير حماية البيانات ضمن تطوير وتشغيل الأنظمة والعمليات منذ المراحل الأولى.

This includes:

ويشمل ذلك:

- Limiting the collection of personal data to what is necessary.
 - Implementing technical and organizational safeguards to protect personal data.
 - Restricting access to personal data to authorized personnel only.
 - Ensuring systems are configured to protect privacy by default.
 - Conducting Data Protection Impact Assessments (DPIAs) when new systems or high-risk processing activities are introduced
- When new technologies, systems, or healthcare services are implemented, the Care Hospitals ensures that privacy risks are assessed and mitigated before the processing begins.

- تقييد جمع البيانات الشخصية بما هو ضروري فقط.
- تطبيق ضوابط فنية وتنظيمية لحماية البيانات الشخصية.
- قصر الوصول إلى البيانات الشخصية على الأشخاص المخولين فقط.
- ضمان إعداد الأنظمة بشكل يحمي الخصوصية بشكل افتراضي.
- إجراء تقييمات أثر حماية البيانات عند إدخال أنظمة جديدة أو أنشطة معالجة عالية المخاطر. وعند تطبيق تقنيات أو أنظمة أو خدمات صحية جديدة، تضمن مستشفيات رعاية تقييم مخاطر الخصوصية ومعالجتها قبل بدء عملية المعالجة.

2.Scope and Applicability

٢.النطاق وقابلية التطبيق

This chapter defines the scope of the Internal Data Protection and Privacy Policy and clarifies how the policy applies within National Medical Care Company, its branches, and its subsidiaries.

يُحدد هذا الفصل نطاق سياسة حماية البيانات والخصوصية الداخلية، ويوضح كيفية تطبيقها داخل الشركة الوطنية للرعاية الطبية وفروعها و شركاتها التابعة . وتضع هذه السياسة الإطار الذي تضمن من خلاله الشركة معالجة البيانات الشخصية بما يتوافق مع نظام حماية البيانات الشخصية في المملكة العربية السعودية ولوائحه التنفيذية.

The policy establishes the framework through which the company ensures that personal data is processed in accordance with the Kingdom of Saudi Arabia Personal Data Protection Law (KSA PDPL) and it's Implementing Regulations.

تنطبق هذه السياسة على جميع البيانات الشخصية التي تتم معالجتها من قبل الشركة ضمن عملياتها الصحية وأنشطتها الإدارية. كما توفر إرشادات للموظفين والأشخاص المخولين بشأن الطريقة المناسبة للتعامل مع البيانات الشخصية وحمايتها وإدارتها طوال دورة حياتها.

The policy applies to all personal data processed by National Medical Care the company, its branches, and its subsidiaries as part of its healthcare operations and administrative activities. It provides guidance to employees and authorized personnel on the appropriate handling, protection, and management of personal data throughout its lifecycle.

٢,١ نطاق تغطية السياسة

2.1 Policy Coverage

This policy applies to all personal data processed by National Medical Care Company, its branches, and its subsidiaries regardless of the form in which the data exists. Personal data may be processed through electronic systems, clinical applications, physical records, communication platforms, or surveillance systems.

تنطبق هذه السياسة على جميع البيانات الشخصية التي تتم معالجتها من قبل الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة، بغض النظر عن الشكل الذي توجد به البيانات. وقد تتم معالجة البيانات الشخصية من خلال الأنظمة الإلكترونية، أو التطبيقات السريرية، أو السجلات الورقية، أو منصات الاتصال، أو أنظمة المراقبة.

The policy governs the entire lifecycle of personal data processing within National Medical Care the company, its branches, and its subsidiaries, including its collection, recording, storage, use, sharing, retention, and destruction or anonymization.

All departments and operational units within the company, its branches, and its subsidiaries must ensure that personal data handled within their activities complies with the principles and requirements outlined in this policy.

2.2 Applicable Entities and Activities

This policy applies across all operational and administrative functions of National Medical Care Company, its branches, and its subsidiaries.

Personal data is processed as part of a wide range of activities necessary for healthcare delivery and organizational operations.

These activities include, but are not limited to, patient registration, medical treatment and clinical documentation, appointment scheduling, insurance and billing processes, workforce management, recruitment, vendor management, facility access control, visitor management, and regulatory reporting. All departments responsible for such activities must ensure that personal data is handled in accordance with this policy and applicable legal requirements.

2.3 Personal Data and Data Subjects

The provisions of this policy apply to personal data relating to individuals who interact with National Medical Care Company, its branches, and its subsidiaries in different capacities. These individuals are referred to as data subjects under the KSA PDPL.

Within National Medical Care Company, its branches, and its subsidiaries, personal data may relate to patients receiving medical services, family members or guardians involved in patient care, employees and medical staff, job applicants, contractors and consultants, vendors and service providers, as well as visitors accessing National Medical Care Company, its branches, and its subsidiaries facilities.

وتحكم هذه السياسة دورة الحياة الكاملة لمعالجة البيانات الشخصية داخل الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة ، بما في ذلك جمعها وتسجيلها وتخزينها واستخدامها ومشاركتها والاحتفاظ بها وإتلافها أو إخفاء هويتها.

ويتعين على جميع الإدارات والوحدات التشغيلية داخل الشركة ضمان أن تتوافق معالجة البيانات الشخصية ضمن أنشطتها مع المبادئ والمتطلبات الواردة في هذه السياسة.

٢,٢ الجهات والأنشطة المشمولة

تنطبق هذه السياسة على جميع الوظائف التشغيلية والإدارية في الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة، حيث تتم معالجة البيانات الشخصية كجزء من مجموعة واسعة من الأنشطة اللازمة لتقديم خدمات الرعاية الصحية وتشغيل المنشأة. وتشمل هذه الأنشطة، على سبيل المثال لا الحصر، تسجيل المرضى، وتقديم العلاج الطبي والتوثيق السريري، وجدولة المواعيد، وإجراءات التأمين والفوترة، وإدارة الموارد البشرية، والتوظيف، وإدارة الموردين، والتحكم في الدخول إلى المرافق، وإدارة الزوار، وإعداد التقارير التنظيمية. ويجب على جميع الإدارات المسؤولة عن هذه الأنشطة التأكد من أن البيانات الشخصية تعالج وفقاً لهذه السياسة والمتطلبات النظامية ذات الصلة.

٢,٣ البيانات الشخصية وأصحاب البيانات

تنطبق أحكام هذه السياسة على البيانات الشخصية المتعلقة بالأفراد الذين يتعاملون مع الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة بصفات مختلفة، ويُشار إلى هؤلاء الأفراد بمصطلح "أصحاب البيانات" وفقاً لنظام حماية البيانات الشخصية في المملكة العربية السعودية.

وقد تشمل البيانات الشخصية داخل لشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة بيانات المرضى الذين يتلقون الخدمات الطبية، وأفراد أسرهم أو أولياء أمورهم المشاركين في الرعاية، والموظفين والكوادر الطبية، والمتقدمين للوظائف، والمتعاقدين والاستشاريين، والموردين ومقدمي الخدمات، بالإضافة إلى الزوار الذين يدخلون مرافق الشركة.

Because National Medical Care Company, its branches, and its subsidiaries operates as a healthcare organization, it frequently processes sensitive personal data, particularly health and medical information.

Such data requires enhanced safeguards and must be handled in strict accordance with the legal requirements governing sensitive personal data under the PDPL.

2.4 Audience and Responsibility

This policy applies to all individuals who process or have access to personal data within National Medical Care Company, its branches, and its subsidiaries. This includes employees, medical staff, administrative personnel, contractors, consultants, trainees, and third-party service providers who may process personal data on behalf of National Medical Care Company, its branches, and its subsidiaries.

All personnel are responsible for ensuring that personal data is handled securely, confidentially, and only for authorized purposes. Individuals who access personal data must follow the procedures and controls established in this policy and any related data protection procedures issued by National Medical Care Company, its branches, and its subsidiaries.

Management within National Medical Care Company, its branches, and its subsidiaries is responsible for ensuring that appropriate controls, training, and oversight mechanisms are implemented to support compliance with this policy and applicable data protection laws. Any suspected misuse of personal data or potential data protection incident must be reported immediately in accordance with the company internal incident management procedures.

وبحكم عمل الشركة الوطنية للرعاية الطبية وفروعها وشركاتها التابعة كمؤسسة صحية، فإنها تعالج بشكل متكرر بيانات شخصية حساسة، لا سيما المعلومات الصحية والطبية.

وتتطلب هذه البيانات تطبيق تدابير حماية معززة، ويجب التعامل معها بما يتوافق بشكل صارم مع المتطلبات النظامية الخاصة بالبيانات الشخصية الحساسة بموجب نظام حماية البيانات الشخصية.

٢,٤ الفئة المستهدفة والمسؤوليات

تنطبق هذه السياسة على جميع الأفراد الذين يقومون بمعالجة البيانات الشخصية أو لديهم صلاحية الوصول إليها داخل الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة، ويشمل ذلك الموظفين، والكوادر الطبية، والموظفين الإداريين، والمتقاعدين، والاستشاريين، والمتدربين، ومقدمي الخدمات من الأطراف الثالثة ذات العلاقة الذين قد يعالجون البيانات الشخصية نيابة عن الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة.

ويقع على عاتق جميع الأفراد مسؤولية ضمان التعامل مع البيانات الشخصية بشكل آمن وسري، وعدم استخدامها إلا للأغراض المصرح بها. كما يجب على كل من لديه صلاحية الوصول إلى البيانات الشخصية الالتزام بالإجراءات والضوابط المنصوص عليها في هذه السياسة وأي إجراءات حماية بيانات أخرى صادرة عن الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة.

وتتحمل إدارة الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة مسؤولية التأكد من تطبيق الضوابط المناسبة، وتوفير التدريب، وتفعيل آليات الرقابة اللازمة لدعم الالتزام بهذه السياسة والأنظمة ذات الصلة بحماية البيانات. كما يجب الإبلاغ فوراً عن أي إساءة استخدام مشتبهاً بها للبيانات الشخصية أو أي حادثة محتملة تتعلق بحماية البيانات، وذلك وفقاً لإجراءات إدارة الحوادث الداخلية المعتمدة لدى الشركة.

3. Definitions

To ensure consistent understanding and application of this policy across National Medical Care Company, its branches, and its subsidiaries, the following key terms are defined in accordance with the Kingdom of Saudi Arabia Personal Data Protection Law (KSA PDPL) and its Implementing Regulations.

These definitions are used throughout this policy to clarify the roles, responsibilities, and concepts related to personal data protection.

٣. التعريفات

لضمان الفهم والتطبيق المتسق لهذه السياسة في الشركة الوطنية للرعاية الطبية وفروعها وشركاتها التابعة يتم تعريف المصطلحات الرئيسية التالية وفقاً لنظام حماية البيانات الشخصية في المملكة العربية السعودية ولوائحه التنفيذية.

وتستخدم هذه التعريفات في جميع أجزاء هذه السياسة لتوضيح الأدوار والمسؤوليات والمفاهيم المرتبطة بحماية البيانات الشخصية.

Terms المصطلحات	Definitions التعريفات
National Medical Care Company, its branches, and its subsidiaries. الشركة الوطنية للرعاية الطبية وفروعها وشركاتها التابعة	National Medical Care Company, its branches, and its subsidiaries Company is the healthcare organization responsible for providing medical services and managing healthcare facilities. For the purposes of this policy, National Medical Care Company, its branches, and its subsidiaries acts as the Data Controller for personal data processed within its healthcare, administrative, and operational activities. الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة هي الجهة الصحية المسؤولة عن تقديم الخدمات الطبية وإدارة مرافق الرعاية الصحية. ولأغراض هذه السياسة، تعد الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة هي المتحكم في البيانات فيما يتعلق بالبيانات الشخصية التي تتم معالجتها ضمن أنشطتها الصحية والإدارية والتشغيلية.
Personal Data البيانات الشخصية	Any information relating to an identified or identifiable individual. An individual may be identified directly or indirectly through identifiers such as name, identification number, location data, online identifier, or through one or more factors related to the individual's physical, physiological, genetic, mental, economic, cultural, or social identity. أي معلومات تتعلق بفرد مُعرف أو يمكن التعرف عليه. ويمكن التعرف على الفرد بشكل مباشر أو غير مباشر من خلال معرفات مثل الاسم أو رقم الهوية أو بيانات الموقع أو المعرف الإلكتروني، أو من خلال عامل أو أكثر يرتبط بهويته الجسدية أو الفسيولوجية أو الجينية أو العقلية أو الاقتصادية أو الثقافية أو الاجتماعية.
Sensitive Personal Data	Personal data that requires enhanced protection under the KSA PDPL due to its sensitive nature. This includes data relating to health status, medical records, genetic or biometric data used for identification, racial or ethnic

Terms المصطلحات	Definitions التعريفات
البيانات الشخصية الحساسة	origin, religious or intellectual beliefs, criminal records, and any data indicating that one or both of the individual's parents are unknown. Within National Medical Care Company, its branches, and its subsidiaries, sensitive personal data commonly includes patient medical records, laboratory results, diagnostic information, and other healthcare-related information. البيانات الشخصية الحساسة: هي البيانات الشخصية التي تتطلب مستوى أعلى من الحماية بموجب نظام حماية البيانات الشخصية في المملكة العربية السعودية نظرًا لطبيعتها الحساسة. وتشمل البيانات المتعلقة بالحالة الصحية، والسجلات الطبية، والبيانات الجينية أو البيومترية المستخدمة للتعرف على الهوية، والأصل العرقي أو الإثني، والمعتقدات الدينية أو الفكرية، والسجلات الجنائية، وأي بيانات تدل على أن أحد والدي الفرد أو كليهما غير معروفين. وفي الشركة الوطنية للرعاية الطبية وفروعها وشركاتها التابعة، تشمل البيانات الشخصية الحساسة بشكل شائع السجلات الطبية للمرضى، ونتائج الفحوصات المخبرية، والمعلومات التشخيصية، وغيرها من المعلومات المتعلقة بالرعاية الصحية.
Data Subject صاحب البيانات	The natural person to whom personal data relates. Within the context of National Medical Care Company, its branches, and its subsidiaries, data subjects may include patients, patient family members or guardians, employees, medical staff, job applicants, contractors, vendors, and visitors. الشخص الطبيعي الذي تتعلق به البيانات الشخصية. وفي سياق الشركة الوطنية للرعاية الطبية وفروعها وشركاتها التابعة، قد يشمل ذلك المرضى، وأفراد أسر المرضى أو أولياء أمورهم، والموظفين، والكوادر الطبية، والمتقدمين للوظائف، والمتعاقدين، والموردين، والزوار.
Processing المعالجة	Any operation or set of operations performed on personal data, whether by automated means or manually. Processing may include collection, recording, organization, storage, retrieval, use, disclosure, sharing, transfer, restriction, deletion, or destruction of personal data. أي عملية أو مجموعة عمليات تُجرى على البيانات الشخصية سواء بوسائل آلية أو يدوية. وتشمل المعالجة جمع البيانات، وتسجيلها، وتنظيمها، وتخزينها، واسترجاعها، واستخدامها، والإفصاح عنها، ومشاركتها، ونقلها، وتقييدها، وحذفها، أو إتلافها.

Terms المصطلحات	Definitions التعريفات
Data Controller المتحكم في البيانات	The entity that determines the purpose and means of processing personal data. For the purposes of this policy, National Medical Care Company, its branches, and its subsidiaries acts as the Data Controller when determining how and why personal data is processed within its operations. الجهة التي تحدد الغرض من معالجة البيانات الشخصية ووسائلها، ولأغراض هذه السياسة تعمل الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة بصفتها المتحكم في البيانات عند تحديد كيفية وأسباب معالجة البيانات الشخصية ضمن عملياتها.
Data Processor معالج البيانات	Any natural or legal person or organization that processes personal data on behalf of the Data Controller in accordance with the controller's instructions. أي شخص طبيعي أو اعتباري أو جهة تقوم بمعالجة البيانات الشخصية نيابة عن المتحكم في البيانات ووفقًا لتعليماته.
Data Breach اختراق البيانات	A security incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data that is processed by National Medical Care Company, its branches, and its subsidiaries . حادث أمني يؤدي إلى الإلحاق العرضي أو غير النظامي، أو الفقد، أو التعديل، أو الإفصاح غير المصرح به، أو الوصول غير المصرح به إلى البيانات الشخصية التي تتم معالجتها من قبل الشركة.
Processing يعالج	Any operation performed on personal data, whether automated or manual, including collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment, combination, restriction, erasure, or destruction. أي عملية يتم إجراؤها على البيانات الشخصية، سواء كانت آلية أو يدوية، بما في ذلك الجمع والتسجيل والتنظيم والهيكلية والتخزين والتكييف والاسترجاع والاستشارة والاستخدام والإفصاح عن طريق الإرسال أو النشر أو الإتاحة بأي شكل آخر، والمواءمة والدمج والتقييد والمحو أو التدمير.

Terms المصطلحات	Definitions التعريفات
Record of Processing Activities (RoPA) سجل أنشطة المعالجة	A documented inventory maintained by National Medical Care Company, its branches, and its subsidiaries that records all personal data processing activities conducted by the organization. The RoPA provides transparency regarding the categories of personal data processed, the purposes of processing, the systems used, and the parties with whom data may be shared. سجل موثق تحتفظ به الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة يتضمن جميع أنشطة معالجة البيانات الشخصية التي تقوم بها. ويوفر هذا السجل شفافية حول فئات البيانات المعالجة، وأغراض المعالجة، والأنظمة المستخدمة، والأطراف التي قد تتم مشاركة البيانات معها.
Data Protection Impact Assessment (DPIA) تقييم أثر حماية البيانات	A structured process used to identify and assess risks to personal data when new processing activities, technologies, or systems are introduced. A DPIA helps ensure that privacy risks are identified and mitigated before processing begins. عملية منظمة تستخدم لتحديد وتقييم المخاطر المتعلقة بالبيانات الشخصية عند إدخال أنشطة معالجة أو تقنيات أو أنظمة جديدة، بما يضمن التعرف على مخاطر الخصوصية ومعالجتها قبل بدء المعالجة.
Anonymization إخفاء الهوية	The process of modifying personal data so that the individual cannot be identified directly or indirectly. Once data has been properly anonymized, it can no longer be associated with a specific individual. عملية تعديل البيانات الشخصية بحيث لا يمكن التعرف على الفرد بشكل مباشر أو غير مباشر. وبعد إتمام إخفاء الهوية بشكل صحيح، لا يمكن ربط البيانات بأي شخص محدد.
Competent Authority الجهة المختصة	The regulatory authority responsible for supervising compliance with the Personal Data Protection Law in the Kingdom of Saudi Arabia. Currently, this role is performed by the Saudi Data and Artificial Intelligence Authority (SDAIA). الجهة التنظيمية المسؤولة عن الإشراف على الالتزام بنظام حماية البيانات الشخصية في المملكة العربية السعودية، وهي حاليًا الهيئة السعودية للبيانات والذكاء الاصطناعي (سدأيا).

٤. البيانات الشخصية التي يتم جمعها

تقوم الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة بجمع ومعالجة البيانات الشخصية كجزء من تقديم خدمات الرعاية الصحية، وإدارة الأنشطة التشغيلية، والوفاء بالالتزامات التنظيمية. وتحرص الشركة على أن يتم جمع ومعالجة البيانات الشخصية بطريقة نظامية وشفافة، وذلك وفقا لنظام حماية البيانات الشخصية في المملكة العربية السعودية ولوائح التنفيذ.

ولا يتم جمع البيانات الشخصية إلا عند الضرورة لدعم تقديم الخدمات الصحية، أو العمليات الإدارية، أو الامتثال للمتطلبات القانونية والتنظيمية. كما تطبق الشركة مبدأ تقليل البيانات، بحيث يتم جمع ومعالجة الحد الأدنى فقط من البيانات الشخصية اللازمة لتحقيق غرض محدد.

٤.١ قائمة أنواع البيانات التي يتم جمعها

تقوم الشركة الوطنية للرعاية الطبية وفروعها والشركات التابعة لها بمعالجة البيانات الشخصية المتعلقة بعدة فئات من الأفراد الذين يتعاملون مع المنشأة. ويعتمد نوع البيانات التي يتم جمعها على طبيعة العلاقة بين الفرد والشركة الوطنية للرعاية الطبية وفروعها والشركات التابعة لها.

المرضى

كجزء من تقديم الرعاية الطبية والخدمات الصحية، تقوم الشركة الوطنية للرعاية الطبية وفروعها والشركات التابعة لها بجمع ومعالجة البيانات الشخصية والبيانات الشخصية الحساسة المتعلقة بالمرضى. وقد يشمل ذلك ما يلي:

- بيانات التعريف الشخصية مثل الاسم، ورقم الهوية الوطنية أو الإقامة، ورقم جواز السفر، وتاريخ الميلاد، والجنس، والجنسية، وبيانات التواصل.
- معلومات التواصل مثل العنوان، ورقم الهاتف، والبريد الإلكتروني.
- المعلومات الطبية والصحية بما في ذلك التاريخ الطبي، والتشخيصات، وسجلات العلاج، ونتائج المختبرات، وتقارير الأشعة، والوصفات الطبية، وغيرها من السجلات السريرية.
- معلومات المواعيد، وسجلات الدخول والخروج من

Data Protection and Privacy Policy

4. Personal Data Collected

National Medical Care Company, its branches, and its subsidiaries collect and process personal data as part of delivering healthcare services, managing operational activities, and fulfilling regulatory obligations. The company ensures that personal data is collected and processed in a transparent and lawful manner in accordance with the Kingdom of Saudi Arabia Personal Data Protection Law (KSA PDPL) and its Implementing Regulations.

Personal data is collected only when necessary to support healthcare delivery, administrative operations, or compliance with legal and regulatory requirements. The company applies the principle of data minimization, meaning that only the personal data required for a specific purpose is collected and processed.

4.1 List of Types of Data Collected

National Medical Care Company, its branches, and its subsidiaries process personal data relating to several categories of individuals who interact with the organization. The type of data collected depends on the relationship between the individual and National Medical Care Company, its branches, and its subsidiaries.

Patients

As part of providing medical care and healthcare services, National Medical Care Company, its branches, and its subsidiaries collect and process personal and sensitive personal data relating to patients. This may include:

- Personal identification details such as name, national ID or Iqama number, passport number, date of birth, gender, nationality, and contact information.
- Contact information such as address, phone number, and email address.
- Medical and health information including medical history, diagnoses, treatment records, laboratory results, radiology reports, prescriptions, and other clinical records.

- Appointment information, admission and discharge records, and treatment schedules.
- Insurance and billing information required for claims processing and financial administration.

Because healthcare services require the processing of medical information, patient records often contain sensitive personal data, which is handled with enhanced safeguards and strict access controls.

Employees and Medical Staff

National Medical Care Company, its branches, and its subsidiaries processes personal data relating to employees and medical professionals working within the organization. This may include:

- Personal identification details such as name, national ID or Iqama, passport details, date of birth, gender, and contact information.
- Employment information including job title, department, employment contract details, and employment history.
- Educational background, professional certifications, licenses, and training records.
- Payroll and financial information necessary for salary payments and benefits administration.
- Attendance records, access logs, and internal system usage records.

In certain cases, limited health-related information may be processed for occupational health, workplace safety, or medical leave management.

Job Applicants

During recruitment activities, National Medical Care Company, its branches, and its subsidiaries collect personal data from job applicants to assess their suitability for employment. This may include:

- Name and contact details.
- Curriculum vitae (CV) or resume.
- Educational qualifications and professional certifications.
- Previous employment history.
- References or recommendation details.

- المستشفى، وجداول العلاج.
- معلومات التأمين والفوترة المطلوبة لمعالجة المطالبات والإدارة المالية.

ونظرًا لأن خدمات الرعاية الصحية تتطلب معالجة المعلومات الطبية، فإن سجلات المرضى غالبًا ما تحتوي على بيانات شخصية حساسة يتم التعامل معها من خلال ضوابط حماية معززة وصلاحيات وصول صارمة.

الموظفون والكوادر الطبية

تقوم الشركة الوطنية للرعاية الطبية وفروعها والشركات التابعة لها بمعالجة البيانات الشخصية المتعلقة بالموظفين والمهنيين الصحيين العاملين لديها، والتي قد تشمل ما يلي:

- بيانات التعريف الشخصية مثل الاسم، ورقم الهوية الوطنية أو الإقامة، وبيانات جواز السفر، وتاريخ الميلاد، والجنس، وبيانات الاتصال.
- معلومات التوظيف مثل المسمى الوظيفي، والقسم، وتفاصيل عقد العمل، والسجل الوظيفي.
- المؤهلات العلمية، والشهادات المهنية، والترخيص، وسجلات التدريب.
- معلومات الرواتب والبيانات المالية اللازمة لصرف الأجور وإدارة المزايا.
- سجلات الحضور والانصراف، وسجلات الدخول إلى الأنظمة، وسجلات استخدام الأنظمة الداخلية.
- في بعض الحالات، قد تتم معالجة معلومات صحية محدودة لأغراض الصحة المهنية، أو السلامة في مكان العمل، أو إدارة الإجازات المرضية.

المتقدمون للوظائف

خلال أنشطة التوظيف، تقوم الشركة الوطنية للرعاية الطبية وفروعها والشركات التابعة لها بجمع البيانات الشخصية من المتقدمين للوظائف لتقييم مدى ملاءمتهم للعمل، وقد يشمل ذلك:

- الاسم وبيانات الاتصال.
- السيرة الذاتية.
- المؤهلات العلمية والشهادات المهنية.
- الخبرات الوظيفية السابقة.
- بيانات المراجع أو التوصيات.

Vendors, Contractors, and Service Providers

National Medical Care Company, its branches, and its subsidiaries may collect personal data relating to representatives of vendors, contractors, and service providers engaged by the organization. This may include:

- Name and contact information of company representatives.
- Job titles and professional roles.
- Business contact details.
- Identification information required for compliance, facility access, or contractual purposes.

Visitors

For facility management and security purposes, the company may collect limited personal data from visitors entering its premises. This may include:

- Name and identification information.
- Contact details when required for visitor registration.
- Records of entry and exit from the company facilities.
- CCTV recordings captured within NMC the company premises for safety and security purposes.

4.2 Why Data is Being Collected

National Medical Care Company, its branches, and its subsidiaries collect and processes personal data to support its core mission of delivering safe and effective healthcare services while maintaining efficient operational management.

Personal data is primarily used to provide medical care and treatment to patients, maintain accurate medical records, manage appointments, and facilitate communication between patients and healthcare professionals.

الموردون والمقاولون ومقدمو الخدمات

قد تقوم الشركة بجمع بيانات شخصية تتعلق بممثلي الموردين والمقاولين ومقدمي الخدمات المتعاقدين معها، وقد يشمل ذلك:

- اسم وبيانات الاتصال الخاصة بممثلي الشركات.
- المسميات الوظيفية والأدوار المهنية.
- بيانات الاتصال الخاصة بالأعمال.
- معلومات التعريف المطلوبة لأغراض الامتثال، أو الدخول إلى المرافق، أو لأغراض تعاقدية.

الزوار

لأغراض إدارة المرافق وتعزيز الأمن، قد تقوم الشركة بجمع بيانات شخصية محدودة من الزوار الداخلين إلى منشأتها، وقد يشمل ذلك:

- الاسم وبيانات التعريف
- بيانات الاتصال عند الحاجة لتسجيل الزوار
- سجلات الدخول والخروج من مرافق الشركة
- تسجيلات كاميرات المراقبة داخل مرافق الشركة لأغراض السلامة والأمن

٤,٢ لماذا يتم جمع البيانات

تقوم الشركة الوطنية للرعاية الطبية وفروعها والشركات التابعة لها بجمع ومعالجة البيانات الشخصية لدعم رسالتها الأساسية في تقديم خدمات رعاية صحية آمنة وفعالة، مع الحفاظ على كفاءة الإدارة التشغيلية.

تستخدم البيانات الشخصية بشكل أساسي لتقديم الرعاية الطبية والعلاج للمرضى، والحفاظ على السجلات الطبية الدقيقة، وإدارة المواعيد، وتسهيل التواصل بين المرضى والمختصين في الرعاية الصحية.

In addition, personal data is processed to support administrative functions such as insurance claims processing, billing management, workforce administration, recruitment processes, and vendor management. National Medical Care Company, its branches, and its subsidiaries may also process personal data to meet legal and regulatory requirements, including reporting obligations to regulatory authorities.

Personal data may also be used to maintain the safety and security of National Medical Care Company, its branches, and its subsidiaries facilities and systems, including managing access to premises and monitoring security systems.

4.3 How Data is Being Collected

National Medical Care Company, its branches, and its subsidiaries collect personal data through several lawful and transparent methods depending on the nature of the interaction with the individual.

In many cases, personal data is collected directly from the data subject. For example, patients provide personal and medical information during registration, consultation, or treatment. Employees and job applicants provide personal data during recruitment and employment processes.

Personal data may also be collected through internal systems and operational platforms used within National Medical Care Company, its branches, and its subsidiaries, including healthcare information systems, appointment management systems, human resources systems, and other administrative applications used to support healthcare services.

In certain situations, personal data may be obtained from authorized third parties, such as insurance providers, recruitment agencies, regulatory bodies, or other healthcare providers when required for lawful purposes.

بالإضافة إلى ذلك، تتم معالجة البيانات الشخصية لدعم الوظائف الإدارية مثل معالجة مطالبات التأمين، وإدارة الفوترة، وإدارة شؤون الموظفين، وإجراءات التوظيف، وإدارة الموردين. كما قد تقوم الشركة الوطنية للرعاية الطبية وفروعها والشركات التابعة لها بمعالجة البيانات الشخصية للوفاء بالمتطلبات النظامية والتنظيمية، بما في ذلك التزامات الإبلاغ للجهات التنظيمية.

وقد تستخدم البيانات الشخصية أيضًا للحفاظ على سلامة وأمن مرافق وأنظمة الشركة الوطنية للرعاية الطبية وفروعها والشركات التابعة لها، بما في ذلك إدارة الدخول إلى المرافق ومراقبة الأنظمة الأمنية.

٤,٣ كيفية جمع البيانات

تقوم الشركة الوطنية للرعاية الطبية وفروعها والشركات التابعة لها بجمع البيانات الشخصية من خلال عدة وسائل نظامية وشفافة، وذلك بحسب طبيعة العلاقة أو التفاعل مع الفرد.

في العديد من الحالات، يتم جمع البيانات الشخصية مباشرة من صاحب البيانات. فعلى سبيل المثال، يقوم المرضى بتقديم بياناتهم الشخصية والطبية أثناء التسجيل أو الاستشارة أو تلقي العلاج. كما يقدم الموظفون والمتقدمون للوظائف بياناتهم الشخصية خلال عمليات التوظيف وإجراءات العمل.

وقد يتم أيضًا جمع البيانات الشخصية من خلال الأنظمة الداخلية والمنصات التشغيلية المستخدمة داخل الشركة الوطنية للرعاية الطبية وفروعها والشركات التابعة لها، بما في ذلك أنظمة المعلومات الصحية، وأنظمة إدارة المواعيد، وأنظمة الموارد البشرية، وغيرها من التطبيقات الإدارية المستخدمة لدعم خدمات الرعاية الصحية.

وفي بعض الحالات، قد يتم الحصول على البيانات الشخصية من أطراف ثالثة مخولة، مثل شركات التأمين، ووكالات التوظيف، والجهات التنظيمية، أو مقدمي الرعاية الصحية الآخرين، وذلك عند الحاجة ولأغراض نظامية مشروعة.

National Medical Care Company, its branches, and its subsidiaries may also collect limited information through automated systems, including system access logs and CCTV systems installed within National Medical Care Company, its branches, and its subsidiaries facilities for security and operational monitoring.

National Medical Care Company, its branches, and its subsidiaries ensures that individuals are informed about how their personal data will be collected and used through appropriate privacy notices and communication channels.

5. Legal Basis for Data Processing

National Medical Care Company, its branches, and its subsidiaries processes personal data only when there is a lawful basis for doing so under the Kingdom of Saudi Arabia Personal Data Protection Law (KSA PDPL) and it's Implementing Regulations.

All processing activities carried out by National Medical Care Company, its branches, and its subsidiaries must be justified by one or more lawful grounds, ensuring that personal data is handled transparently, fairly, and in accordance with applicable legal requirements.

Given the nature of healthcare services, National Medical Care Company, its branches, and its subsidiaries frequently processes sensitive personal data, particularly medical and health information. Such processing is carried out only when it is necessary for providing healthcare services, fulfilling legal obligations, or protecting the interests of individual.

5.1 Consent

In certain situations, National Medical Care Company, its branches, and its subsidiaries processes personal data based on the consent of the data subject. Consent must be freely given, clear, and informed. Individuals must understand the purpose for which their data is being collected and how it will be used.

كما قد تقوم الشركة الوطنية للرعاية الطبية وفروعها والشركات التابعة لها بجمع معلومات محدودة من خلال الأنظمة الآلية، بما في ذلك سجلات الدخول إلى الأنظمة وتسجيلات كاميرات المراقبة المثبتة داخل مرافق الشركة الوطنية للرعاية الطبية وفروعها والشركات التابعة لها، وذلك لأغراض الأمن والمراقبة التشغيلية.

وتحرص الشركة الوطنية للرعاية الطبية وفروعها والشركات التابعة لها على إبلاغ الأفراد بكيفية جمع بياناتهم الشخصية واستخدامها من خلال إشعارات الخصوصية المناسبة وقنوات التواصل المعتمدة.

٥. الأساس القانوني لمعالجة البيانات

تقوم الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة بمعالجة البيانات الشخصية فقط عند وجود أساس نظامي يجيز ذلك، وذلك وفقاً لنظام حماية البيانات الشخصية في المملكة العربية السعودية ولوائح التنفيذ.

ويجب أن تستند جميع أنشطة المعالجة التي تقوم بها الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة إلى أساس نظامي واحد أو أكثر، بما يضمن التعامل مع البيانات الشخصية بشكل شفاف وعادل ومتوافق مع المتطلبات النظامية.

ونظراً لطبيعة خدمات الرعاية الصحية، فإن الشركة تقوم بشكل متكرر بمعالجة بيانات شخصية حساسة، لا سيما المعلومات الطبية والصحية، ويتم ذلك فقط عند الضرورة لتقديم الخدمات الصحية، أو للوفاء بالالتزامات النظامية، أو لحماية مصالح الفرد.

٥.١ الموافقة

في بعض الحالات، تقوم الشركة الوطنية للرعاية الطبية وفروعها والشركات التابعة لها بمعالجة البيانات الشخصية بناءً على موافقة صاحب البيانات، ويجب أن تكون هذه الموافقة صريحة وواضحة ومبنية على علم كامل. كما يجب أن يكون الفرد على دراية بالغرض من جمع بياناته وكيفية استخدامها.

Where consent is used as the legal basis for processing, individuals must be able to withdraw their consent at any time. National Medical Care Company, its branches, and its subsidiaries ensures that withdrawing consent is as easy as providing it. Once consent is withdrawn, the company will stop processing the personal data unless another lawful basis applies.

Consent may be used in situations such as for providing medical services to Patients, voluntary participation in surveys, marketing and advertisement communications, or other activities where consent is required by law.

5.2 Contractual Necessity

Personal data may be processed when it is necessary for the performance of a contract or for taking steps prior to entering a contract with the data subject.

Within National Medical Care Company, its branches, and its subsidiaries, this may include processing personal data to manage employment relationships, process payroll and employee benefits, or manage contracts with vendors and service providers.

Processing may also be required to facilitate certain healthcare services where administrative arrangements are necessary to deliver care.

5.3 Legal Obligation

National Medical Care Company, its branches, and its subsidiaries processes personal data when required to comply with legal or regulatory obligations under applicable laws and regulations within the Kingdom of Saudi Arabia.

This includes obligations related to ministry of health and other healthcare regulations, financial reporting, insurance processing, employment laws, and regulatory reporting to relevant authorities. In such cases, National Medical Care Company, its branches, and its subsidiaries processes personal data only to the extent necessary to meet these legal requirements.

وعند الاعتماد على الموافقة كأساس نظامي للمعالجة، يجب أن يكون بإمكان الأفراد سحب موافقتهم في أي وقت. وتحرص الشركة على أن يكون سحب الموافقة بنفس سهولة تقديمها وعند سحب الموافقة، تتوقف الشركة عن معالجة البيانات الشخصية ما لم يوجد أساس نظامي آخر يجيز ذلك.

وقد تستخدم الموافقة في حالات مثل تقديم الخدمات الطبية للمرضى، المشاركة الطوعية في الاستبيانات، أو الاتصالات التسويقية والإعلانية، أو غيرها من الأنشطة التي يتطلب فيها النظام الحصول على موافقة صريحة.

٥,٢ الضرورة التعاقدية

يجوز معالجة البيانات الشخصية عندما تكون ضرورية لتنفيذ عقد يكون صاحب البيانات طرفاً فيه، أو لاتخاذ خطوات سابقة لإبرام عقد مع صاحب البيانات.

وفي الشركة الوطنية للرعاية الطبية وفروعها وشركاتها التابعة، قد يشمل ذلك معالجة البيانات الشخصية لإدارة علاقات العمل، ومعالجة الرواتب ومزايا الموظفين، أو إدارة العقود مع الموردين ومقدمي الخدمات.

كما قد تكون المعالجة مطلوبة لتسهيل بعض خدمات الرعاية الصحية عندما تكون الترتيبات الإدارية ضرورية لتقديم الرعاية.

٥,٣ الالتزام القانوني

تقوم الشركة الوطنية للرعاية الطبية وفروعها وشركاتها التابعة بمعالجة البيانات الشخصية عند الحاجة إلى الامتثال للالتزامات القانونية أو التنظيمية بموجب الأنظمة واللوائح المعمول بها في المملكة العربية السعودية.

ويشمل ذلك الالتزامات المتعلقة بوزارة الصحة وغيرها من الأنظمة الصحية، والتقارير المالية، ومعالجة التأمين، وأنظمة العمل، والتقارير التنظيمية المقدمة إلى الجهات المختصة. وفي مثل هذه الحالات، تقوم شركة الوطنية للرعاية الطبية وفروعها وشركاتها التابعة بمعالجة البيانات الشخصية فقط بالقدر اللازم للوفاء بهذه المتطلبات القانونية.

٥,٤ حماية المصالح الحيوية

5.4 Protection of Vital Interest

In certain circumstances, personal data may be processed to protect the vital interests of the data subject or another individual. This typically applies in situations where processing is necessary to protect a person's life, health, or physical safety.

In a healthcare environment such as National Medical Care Company, its branches, and its subsidiaries, this may arise during medical emergencies where healthcare professionals must access or process patient data to provide urgent medical treatment.

في بعض الحالات، قد تتم معالجة البيانات الشخصية لحماية المصالح الحيوية لصاحب البيانات أو لشخص آخر. ويُطبق ذلك عادة في الحالات التي تكون فيها المعالجة ضرورية لحماية حياة الشخص أو صحته أو سلامته الجسدية.

وفي بيئة الرعاية الصحية مثل الشركة الوطنية للرعاية الطبية وفروعها وشركاتها التابعة، قد ينشأ ذلك أثناء حالات الطوارئ الطبية، حيث يتعين على مقدمي الرعاية الصحية الوصول إلى بيانات المرضى أو معالجتها لتقديم علاج طبي عاجل.

5.5 Public Interest

٥,٥ المصلحة العامة

Personal data may be processed where it is necessary for tasks carried out in the public interest or where National Medical Care Company, its branches, and its subsidiaries is required to fulfil responsibilities that support public health and safety.

This may include processing personal data for regulatory reporting, public health monitoring, compliance with healthcare standards, or cooperation with regulatory authorities where required by law.

قد تتم معالجة البيانات الشخصية عندما يكون ذلك ضروريًا للقيام بمهام تنفذ للمصلحة العامة، أو عندما تكون الشركة الوطنية للرعاية الطبية وفروعها وشركاتها التابعة مُلزَمة بالوفاء بمسؤوليات تدعم الصحة العامة والسلامة العامة.

وقد يشمل ذلك معالجة البيانات الشخصية لأغراض التقارير التنظيمية، أو مراقبة الصحة العامة، أو الامتثال لمعايير الرعاية الصحية، أو التعاون مع الجهات التنظيمية وفقًا لما يقتضيه القانون.

5.6 Pursue legitimate operational interests

٥,٦ تحقيق المصالح التشغيلية المشروعة

In certain situations, National Medical Care Company, its branches, and its subsidiaries may process personal data to pursue legitimate operational interests, provided that such interests do not override the rights and freedoms of the data subject.

Examples may include maintaining the security of National Medical Care Company, its branches, and its subsidiaries facilities and systems, preventing fraud, ensuring operational efficiency, and improving service quality. When relying on legitimate interests, National Medical Care Company, its branches, and its subsidiaries ensures that appropriate safeguards are implemented to protect personal data and the rights of individuals.

في بعض الحالات، قد تقوم الشركة الوطنية للرعاية الطبية وفروعها وشركاتها التابعة بمعالجة البيانات الشخصية لتحقيق مصالح تشغيلية مشروعة، شريطة ألا تتجاوز هذه المصالح حقوق وحريات صاحب البيانات.

قد تشمل الأمثلة الحفاظ على أمن مرافق وأنظمة الشركة الوطنية للرعاية الطبية وفروعها وشركاتها التابعة، ومنع الاحتيال، وضمان الكفاءة التشغيلية، وتحسين جودة الخدمات. وعند الاعتماد على المصالح المشروعة، تضمن الشركة الوطنية للرعاية الطبية وفروعها وشركاتها التابعة تطبيق الضمانات المناسبة لحماية البيانات الشخصية وحقوق الأفراد.

6. Record of Processing Activities (RoPA) & Data Protection Impact Assessment

National Medical Care Company, its branches, and its subsidiaries maintains structured documentation of its personal data processing activities in order to ensure transparency, accountability, and compliance with the Kingdom of Saudi Arabia Personal Data Protection Law (KSA PDPL) and its Implementing Regulations. Proper documentation and risk assessment enable National Medical Care Company, its branches, and its subsidiaries to understand how personal data flows through the organization and to identify potential risks to individuals' privacy.

6.1 Record of Processing Activities (RoPA)

National Medical Care Company, its branches, and its subsidiaries maintains a Record of Processing Activities (RoPA) that documents all personal data processing activities carried out within the organization. The RoPA serves as an internal register that provides visibility over how personal data is collected, used, stored, shared, and retained across different departments and systems.

The RoPA typically includes information such as:

- The purpose of the processing activity
- Categories of personal data processed
- Categories of data subjects involved
- Systems or applications used to process personal data
- Data retention periods
- Third parties with whom personal data may be shared
- Security measures applied to protect personal data

Each department within National Medical Care Company, its branches, and its subsidiaries that processes personal data is responsible for providing accurate and up-to-date information regarding its processing activities. These details are recorded and maintained within the RoPA to ensure that National Medical Care Company, its branches, and its

٦. سجل أنشطة معالجة البيانات وتقييم أثر حماية البيانات

تحتفظ الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة بسجلات موثقة ومنظمة لأنشطة معالجة البيانات الشخصية لديها، وذلك لضمان الشفافية والمساءلة والامتثال لنظام حماية البيانات الشخصية في المملكة العربية السعودية ولوائح التنفيذ.

كما يتيح التوثيق السليم وتقييم المخاطر لشركة الوطنية للرعاية الطبية وفروعها وشركاتها التابعة فهم كيفية تدفق البيانات الشخصية داخل المنظمة، وتحديد المخاطر المحتملة على خصوصية الأفراد.

٦,١ سجل أنشطة المعالجة

تحتفظ الشركة الوطنية للرعاية الطبية وفروعها والشركات التابعة لها بسجل لأنشطة معالجة البيانات الشخصية ، والذي يوثق جميع أنشطة معالجة البيانات الشخصية التي تتم داخل المنشأة. ويعمل هذا السجل كسجل داخلي يوفر رؤية شاملة حول كيفية جمع البيانات الشخصية واستخدامها وتخزينها ومشاركتها والاحتفاظ بها عبر مختلف الإدارات والأنظمة.

ويتضمن سجل أنشطة المعالجة (RoPA) عادة معلومات مثل:

- الغرض من نشاط المعالجة
- فئات البيانات الشخصية التي تتم معالجتها
- فئات أصحاب البيانات المعنيين
- الأنظمة أو التطبيقات المستخدمة لمعالجة البيانات الشخصية
- فترات الاحتفاظ بالبيانات
- الأطراف الثالثة التي قد تتم مشاركة البيانات الشخصية معها
- التدابير الأمنية المطبقة لحماية البيانات الشخصية.

وتتحمل كل إدارة داخل الشركة الوطنية للرعاية الطبية وفروعها وشركاتها التابعة التي تقوم بمعالجة البيانات الشخصية مسؤولية توفير معلومات دقيقة ومحدثة حول أنشطة المعالجة الخاصة بها.

ويتم تسجيل هذه المعلومات والاحتفاظ بها ضمن سجل أنشطة المعالجة لضمان امتلاك الشركة الوطنية للرعاية الطبية وفروعها وشركاتها التابعة رؤية شاملة وكاملة لجميع أنشطة معالجة البيانات

subsidiaries has a complete overview of all personal data processing activities.

The RoPA must be reviewed and updated whenever there are significant changes to processing activities, including the introduction of new systems, services, or data processing purposes.

6.2 Data Protection Impact Assessment

National Medical Care Company, its branches, and its subsidiaries conducts Data Protection Impact Assessments (DPIAs) when a new project, system, or process involving personal data may present a higher risk to the privacy or rights of individuals.

A DPIA helps identify and evaluate potential privacy risks before the processing begins and ensures that appropriate safeguards are implemented to mitigate those risks.

A DPIA may be required in situations such as:

- Processing of sensitive personal data, including health and medical information
- Implementation of new technologies or digital health systems
- Large-scale processing of patient data
- Continuous monitoring of individuals through surveillance systems
- Integration of multiple data sources that may increase privacy risks

The DPIA process allows National Medical Care Company, its branches, and its subsidiaries to assess whether the intended processing complies with data protection requirements and whether additional technical or organizational safeguards are necessary

By maintaining an up-to-date RoPA and conducting DPIAs where appropriate, National Medical Care Company, its branches, and its subsidiaries ensures that personal data processing activities are properly documented, monitored, and managed in accordance with PDPL requirements.

الشخصية.

يجب مراجعة سجل أنشطة المعالجة وتحديثه كلما طرأت تغييرات جوهرية على أنشطة المعالجة، بما في ذلك إدخال أنظمة أو خدمات جديدة، أو استحداث أغراض جديدة لمعالجة البيانات الشخصية.

٦,٢ تقييم أثر حماية البيانات

تقوم الشركة الوطنية للرعاية الطبية وفروعها والشركات التابعة لها بإجراء تقييمات أثر حماية البيانات عند وجود مشروع أو نظام أو إجراء جديد يتضمن معالجة بيانات شخصية وقد يترتب عليه مخاطر مرتفعة على خصوصية الأفراد أو حقوقهم. يساعد تقييم أثر حماية البيانات على تحديد وتقييم المخاطر المحتملة المتعلقة بالخصوصية قبل بدء المعالجة، كما يضمن تطبيق الضمانات المناسبة للتخفيف من تلك المخاطر.

قد يكون إجراء تقييم أثر حماية البيانات مطلوباً في حالات مثل:

- معالجة البيانات الشخصية الحساسة، بما في ذلك البيانات الصحية والطبية
- تطبيق تقنيات جديدة أو أنظمة صحية رقمية جديدة
- المعالجة واسعة النطاق لبيانات المرضى
- المراقبة المستمرة للأفراد من خلال أنظمة المراقبة
- دمج مصادر بيانات متعددة بما قد يزيد من مخاطر الخصوصية

تتيح عملية تقييم أثر حماية البيانات للشركة الوطنية للرعاية الطبية وفروعها والشركات التابعة لها تقييم مدى توافق المعالجة المقترحة مع متطلبات حماية البيانات، وتحديد ما إذا كانت هناك حاجة إلى ضوابط تقنية أو تنظيمية إضافية.

ومن خلال الاحتفاظ بسجل محدث لأنشطة المعالجة وإجراء تقييمات أثر حماية البيانات عند الحاجة، تضمن الشركة الوطنية للرعاية الطبية وفروعها والشركات التابعة لها أن أنشطة معالجة البيانات الشخصية يتم توثيقها ومراقبتها وإدارتها بالشكل المناسب ووفقاً لمتطلبات نظام حماية البيانات الشخصية.

7. Data Storage and Retention

National Medical Care Company, its branches, and its subsidiaries ensures that personal data is stored securely and retained only for as long as necessary to fulfil the purposes for which it was collected.

All storage and retention practices are aligned with the requirements of the Kingdom of Saudi Arabia Personal Data Protection Law (KSA PDPL), its Implementing Regulations, and other applicable healthcare and regulatory requirements.

National Medical Care Company, its branches, and its subsidiaries maintains a separate Personal Data Retention and Policy that defines detailed retention periods and disposal procedures for different categories of personal data processed by the organization. This policy provides specific guidance on how long personal data must be retained based on legal, regulatory, and operational requirements.

All departments within National Medical Care Company, its branches, and its subsidiaries must follow the requirements of the Personal Data Retention and Disposal Policy when determining how long personal data should be stored and when it should be securely deleted or anonymized.

7.1 Policy Highlights

National Medical Care Company, its branches, and its subsidiaries applies clear principles to ensure responsible storage and retention of personal data. Personal data is retained only for the period necessary to achieve the purpose for which it was collected or to comply with applicable legal and regulatory obligations.

Retention periods are determined based on the nature of the data, the purpose of processing, and relevant legal requirements. Once the purpose for processing has been fulfilled and the applicable retention period has expired, personal data must be securely deleted or anonymized in accordance with approved procedures.

٧. تخزين البيانات والاحتفاظ بها

تضمن الشركة الوطنية للرعاية الطبية وفروعها وشركاتها التابعة تخزين البيانات الشخصية بشكل آمن والاحتفاظ بها فقط للمدة اللازمة لتحقيق الأغراض التي جُمعت من أجلها.

تتوافق جميع ممارسات تخزين البيانات والاحتفاظ بها مع متطلبات نظام حماية البيانات الشخصية في المملكة العربية السعودية ولائحته التنفيذية، بالإضافة إلى المتطلبات التنظيمية والصحية الأخرى ذات الصلة والواجبة التطبيق.

تحتفظ الشركة الوطنية للرعاية الطبية وفروعها وشركاتها التابعة بسياسة مستقلة للاحتفاظ بالبيانات الشخصية وإتلافها، تحدد مدد الاحتفاظ التفصيلية وإجراءات الإتلاف الخاصة بمختلف فئات البيانات الشخصية التي تعالجها الشركة. وتوفر هذه السياسة إرشادات محددة بشأن المدة التي يجب خلالها الاحتفاظ بالبيانات الشخصية استناداً إلى المتطلبات النظامية والتنظيمية والتشغيلية المعمول بها.

يجب على جميع الإدارات في الشركة الوطنية للرعاية الطبية وفروعها وشركاتها التابعة الالتزام بمتطلبات سياسة الاحتفاظ بالبيانات الشخصية وإتلافها عند تحديد مدة الاحتفاظ بالبيانات الشخصية، وكذلك عند اتخاذ الإجراءات اللازمة لحذفها أو إتلافها أو إخفاء هويتها بشكل آمن عند انتهاء الغرض من الاحتفاظ بها أو انقضاء المدة النظامية المقررة لذلك.

٧.١ أبرز أحكام السياسة

تطبق الشركة الوطنية للرعاية الطبية وفروعها وشركاتها التابعة مبادئ واضحة لضمان تخزين البيانات الشخصية والاحتفاظ بها بصورة مسؤولة وآمنة. ويتم الاحتفاظ بالبيانات الشخصية فقط للمدة اللازمة لتحقيق الغرض الذي جُمعت من أجله أو للامتثال للالتزامات النظامية والتنظيمية المعمول بها.

يتم تحديد مدد الاحتفاظ بالبيانات الشخصية بناءً على طبيعة البيانات، والغرض من معالجتها، والمتطلبات النظامية ذات الصلة. وعند تحقيق الغرض من المعالجة وانتهاء مدة الاحتفاظ المقررة، يجب حذف البيانات الشخصية أو إخفاء هويتها بشكل آمن وفقاً للإجراءات المعتمدة.

Access to stored personal data is restricted to authorized personnel who require access for legitimate operational, clinical, or administrative purposes.

كما يقتصر الوصول إلى البيانات الشخصية المخزنة على الموظفين المصرح لهم فقط، والذين تتطلب مهامهم الوصول إليها لأغراض تشغيلية أو سريرية أو إدارية مشروعة.

7.2 Data Storage

٧,٢ تخزين البيانات

Personal data within National Medical Care Company, its branches, and its subsidiaries may be stored in different systems and formats depending on operational requirements. This includes electronic systems such as healthcare information systems, administrative applications, and secure databases, as well as physical records maintained within controlled environments.

قد يتم تخزين البيانات الشخصية داخل الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة باستخدام أنظمة وصيغ مختلفة وفقاً للاحتياجات التشغيلية، ويشمل ذلك الأنظمة الإلكترونية مثل أنظمة المعلومات الصحية، والتطبيقات الإدارية، وقواعد البيانات الآمنة، بالإضافة إلى السجلات الورقية المحفوظة في بيئات خاضعة للرقابة.

National Medical Care Company, its branches, and its subsidiaries ensures that appropriate technical and organizational safeguards are implemented to protect stored personal data. These safeguards include access controls, secure system configurations, encryption where appropriate, and physical security measures for facilities where records are stored.

وتحرص الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة على تطبيق تدابير فنية وتنظيمية مناسبة لحماية البيانات الشخصية المخزنة، مثل ضوابط التحكم في الوصول، وإعدادات الأنظمة الآمنة، وتقنيات التشفير عند الحاجة، إضافة إلى تدابير الحماية المادية للمرافق التي يتم فيها حفظ السجلات.

Where personal data is stored or processed by third-party service providers, National Medical Care Company, its branches, and its subsidiaries ensures that such providers implement appropriate security measures and comply with the data protection obligations established by National Medical Care Company, its branches, and its subsidiaries.

وفي حال تخزين البيانات الشخصية أو معالجتها من قبل أطراف ثالثة، تضمن الشركة أن يلتزم هؤلاء المزودون بتطبيق تدابير أمنية مناسبة والامتثال لمتطلبات حماية البيانات التي تفرضها الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة.

7.3 Data Deletion and Anonymization

٧,٣ حذف البيانات وإخفاء هويتها

When personal data is no longer required for the purpose for which it was collected and the applicable retention period has expired, National Medical Care Company, its branches, and its subsidiaries ensures that the data is securely removed from its systems.

عند عدم الحاجة إلى البيانات الشخصية للغرض الذي جُمعت من أجله، وانتهاء مدة الاحتفاظ المحددة، تضمن الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة إزالة هذه البيانات من أنظمتها بشكل آمن.

Personal data may be securely deleted or anonymized so that individuals can no longer be identified directly or indirectly. These processes are conducted in accordance with the procedures defined in the

وقد يتم حذف البيانات الشخصية بشكل نهائي أو إخفاء هويتها بحيث لا يمكن التعرف على الأفراد بشكل مباشر أو غير مباشر. ويتم تنفيذ هذه العمليات وفقاً للإجراءات المحددة في سياسة الاحتفاظ بالبيانات الخاصة بالشركة، وبما يتوافق مع الإرشادات الصادرة عن

By following these procedures, National Medical Care Company, its branches, and its subsidiaries ensures that personal data is not retained longer than necessary and that it is disposed of in a secure and controlled manner.

8. Data Storage and Retention

National Medical Care Company, its branches, and its subsidiaries may use cookies and similar technologies on its websites or digital platforms to support functionality, improve user experience, and ensure the secure operation of online services. Cookies are small text files that are stored on a user's device when visiting a website. These technologies help the Company understand how users interact with its online services and allow certain features to operate effectively.

Where cookies are used, National Medical Care Company, its branches, and its subsidiaries ensures that their use is consistent with applicable privacy and data protection requirements under the Kingdom of Saudi Arabia Personal Data Protection Law (KSA PDPL).

8.1 Types of Cookies

Cookies used on National Medical Care Company, its branches, and its subsidiaries digital platforms may include the following categories:

- **Essential Cookies**
These cookies are necessary for the operation of the website or digital platform. They enable basic features such as page navigation, secure access to certain areas of the platform, and system functionality.
- **Performance Cookies**
These cookies help National Medical Care the Company, its branches, and its subsidiaries understand how users interact with its website by collecting information such as page visits, navigation patterns, and system performance. The

ومن خلال الالتزام بهذه الإجراءات، تضمن الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة عدم الاحتفاظ بالبيانات الشخصية لفترة أطول من اللازم، والتخلص منها بطريقة آمنة ومنضبطة.

٨. ملفات تعريف الارتباط

قد تستخدم الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة ملفات تعريف الارتباط والتقنيات المشابهة على مواقعها الإلكترونية أو منصاتها الرقمية، وذلك لدعم الوظائف، وتحسين تجربة المستخدم، وضمان التشغيل الآمن للخدمات الإلكترونية. وملفات تعريف الارتباط هي ملفات نصية صغيرة يتم تخزينها على جهاز المستخدم عند زيارة الموقع الإلكتروني، وتساعد هذه التقنيات الشركة على فهم كيفية تفاعل المستخدمين مع خدماتها الرقمية وتمكين بعض الميزات من العمل بكفاءة.

وفي حال استخدام هذه الملفات، تلتزم الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة بأن يكون استخدامها متوافقاً مع متطلبات الخصوصية وحماية البيانات المعمول بها في المملكة العربية السعودية.

٨.١ أنواع ملفات تعريف الارتباط

قد تشمل ملفات تعريف الارتباط المستخدمة على منصات الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة الرقمية الأنواع التالية:

- **ملفات تعريف الارتباط الأساسية**
وهي ملفات ضرورية لتشغيل الموقع أو المنصة الرقمية، حيث تمكن من الوظائف الأساسية مثل التنقل بين الصفحات، والوصول الآمن إلى بعض أجزاء النظام، وتشغيل الخدمات الأساسية.
- **ملفات تعريف الارتباط الخاصة بالأداء**
تساعد هذه الملفات الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة على فهم كيفية تفاعل المستخدمين مع الموقع من خلال جمع معلومات مثل عدد الزيارات، وأنماط التصفح، وأداء النظام. وعادة ما تكون هذه البيانات مجمعة وتستخدم لتحسين كفاءة الخدمات الرقمية.

information collected is typically aggregated and used to improve the functionality of digital services.

- **Functional Cookies**
Functional cookies allow websites to remember certain preferences or settings chosen by the user, such as language preferences or system configuration options, which improves the overall user experience.

8.2 Consent and Control

Where required, users will be informed about the use of cookies when accessing the Company website or digital platforms. Individuals may have the option to accept or manage cookie preferences through website settings or browser controls.

Users can also modify their browser settings to block or delete cookies. However, disabling certain cookies may affect the functionality or performance of some online services.

8.3 Data Collected Through Cookies

Information collected through cookies may include technical data related to website usage, such as IP address, browser type, device information, and pages visited. This information is used primarily to maintain the security and functionality of National Medical Care Company, its branches, and its subsidiaries digital platforms and to improve the overall user experience.

Any personal data collected through cookies is handled in accordance with this policy and applicable data protection requirements.

9. Data Subject Rights

National Medical Care Company, its branches, and its subsidiaries recognizes and respects the rights of individuals regarding the processing of their personal data in accordance with the Kingdom of Saudi Arabia Personal Data Protection Law (KSA PDPL) and its Implementing Regulations. The Company is committed to ensuring transparency in how personal data is

- ملفات تعريف الارتباط الوظيفية

تمكن هذه الملفات المواقع من تذكر تفضيلات المستخدم مثل اللغة أو إعدادات النظام، مما يُحسن تجربة الاستخدام بشكل عام.

٨,٢ الموافقة والتحكم

عند الحاجة، يتم إشعار المستخدمين باستخدام ملفات تعريف الارتباط عند دخولهم إلى موقع الشركة أو منصاتها الرقمية. وقد يُتاح للأفراد خيار الموافقة على استخدام هذه الملفات أو إدارة تفضيلاتهم من خلال إعدادات الموقع أو المتصفح.

كما يمكن للمستخدمين تعديل إعدادات المتصفح لحظر أو حذف ملفات تعريف الارتباط، إلا أن تعطيل بعض هذه الملفات قد يؤثر على أداء بعض الخدمات الإلكترونية أو وظائفها.

٨,٣ البيانات التي يتم جمعها من خلال ملفات تعريف الارتباط

قد تشمل المعلومات التي يتم جمعها من خلال ملفات تعريف الارتباط بيانات تقنية تتعلق باستخدام الموقع الإلكتروني، مثل عنوان بروتوكول الإنترنت، ونوع المتصفح، ومعلومات الجهاز، والصفحات التي تمت زيارتها. ويتم استخدام هذه المعلومات بشكل أساسي للحفاظ على أمن ووظائف المنصات الرقمية التابعة للشركة الوطنية للرعاية الطبية وفروعها وشركاتها التابعة، وتحسين تجربة المستخدم بشكل عام.

ويتم التعامل مع أي بيانات شخصية يتم جمعها من خلال ملفات تعريف الارتباط وفقاً لهذه السياسة والمتطلبات المعمول بها في مجال حماية البيانات.

٩. حقوق أصحاب البيانات

تقر الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة بحقوق الأفراد فيما يتعلق بمعالجة بياناتهم الشخصية، وتحترم هذه الحقوق وفقاً لنظام حماية البيانات الشخصية في المملكة العربية السعودية ولوائحه التنفيذية. وتلتزم الشركة بتوفير الشفافية في كيفية معالجة البيانات، وإتاحة الوسائل التي تمكن الأفراد من ممارسة حقوقهم عند الحاجة.

processed and providing individuals with mechanisms to exercise their rights where applicable.

National Medical Care Company, its branches, and its subsidiaries has established Data Subject Request procedure to ensure that requests related to personal data are handled in a timely and transparent manner while maintaining appropriate safeguards to protect the confidentiality and security of personal information.

9.1 Right to be informed

Individuals have the right to be informed about the purpose for collecting their personal data, the legal basis for processing, and how their personal data will be used. National Medical Care Company, its branches, and its subsidiaries ensures that individuals are provided with clear and transparent information through privacy notices and other relevant communications at the time their personal data is collected.

9.2 Right to Access to Your Personal Data

Individuals have the right to access their personal data that is processed by National Medical Care Company, its branches, and its subsidiaries. Upon receiving a valid request, the company will provide confirmation of whether personal data relating to the individual is being processed and may provide access to that information in accordance with applicable legal requirements.

9.3 Right to Request Access to Obtain Personal Data

Individuals may request a copy of their personal data held by National Medical Care Company, its branches, and its subsidiaries in a readable and clear format. Where applicable, National Medical Care Company, its branches, and its subsidiaries may provide the requested information in a structured and commonly used format, subject to any legal or regulatory limitations.

وقد وضعت الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة إجراءات مخصصة لطلبات أصحاب البيانات، لضمان التعامل مع هذه الطلبات بشكل منظم وفي الوقت المناسب، مع الحفاظ على سرية وأمن المعلومات.

٩,١ الحق في المعرفة

يحق للأفراد معرفة الغرض من جمع بياناتهم الشخصية، والأساس النظامي لمعالجتها، وكيفية استخدامها. وتحرص الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة على تزويد الأفراد بمعلومات واضحة وشفافة من خلال إشعارات الخصوصية ووسائل التواصل ذات الصلة عند جمع البيانات.

٩,٢ الحق في الوصول إلى البيانات الشخصية

يحق للأفراد الوصول إلى بياناتهم الشخصية التي تتم معالجتها من قبل الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة. وعند تقديم طلب صحيح، تقوم الشركة بتأكيد ما إذا كانت تعالج بيانات شخصية تخص الفرد، وقد تتيح له الوصول إلى هذه البيانات وفقاً للمتطلبات النظامية.

٩,٣ الحق في طلب الحصول على البيانات الشخصية

يجوز للأفراد طلب الحصول على نسخة من بياناتهم الشخصية المحفوظ بها لدى الشركة الوطنية للرعاية الطبية وفروعها وشركاتها التابعة بصيغة واضحة ومقروءة. وحيثما ينطبق ذلك، يجوز للشركة الوطنية للرعاية الطبية وفروعها وشركاتها التابعة تزويد المعلومات المطلوبة بصيغة منظمة ومستخدمة على نطاق واسع، وذلك وفقاً لأي قيود نظامية أو تنظيمية معمول بها.

٩,٤ الحق في تصحيح البيانات الشخصية

يحق للأفراد طلب تصحيح بياناتهم الشخصية أو استكمالها أو تحديثها إذا كانت غير دقيقة أو غير مكتملة أو قديمة. وتقوم الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة بمراجعة هذه الطلبات واتخاذ الإجراءات اللازمة لضمان دقة البيانات وتحديثها بشكل مستمر.

9.4 Right to Correct Personal Data

Individuals have the right to request the correction, completion, or updating of their personal data if it is inaccurate, incomplete, or outdated. National Medical Care Company, its branches, and its subsidiaries will review such requests and take appropriate steps to ensure that personal data remains accurate and up to date.

٩,٥ الحق في طلب إتلاف البيانات الشخصية

يحق للأفراد طلب إتلاف بياناتهم الشخصية إذا لم تعد هناك حاجة إلى هذه البيانات للغرض الذي جُمعت أو عُولجت من أجله، وذلك بشرط ألا تكون الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة ملزمة بالاحتفاظ بها بموجب الالتزامات النظامية أو التنظيمية المعمول بها.

9.5 Right to Request Destruction of Personal Data

Individuals may request the destruction of their personal data if the data is no longer necessary for the purpose for which it was collected or processed, provided that National Medical Care Company, its branches, and its subsidiaries is not required to retain the data under applicable legal or regulatory obligations.

٩,٦ الحق في سحب الموافقة

في الحالات التي تعتمد فيها معالجة البيانات الشخصية على الموافقة، يحق للأفراد سحب موافقتهم في أي وقت. وعند سحب الموافقة، تتوقف الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة عن معالجة البيانات الشخصية للغرض المعني، ما لم يوجد أساس نظامي آخر يجيز استمرار المعالجة.

9.6 Right to Withdraw Consent

Where personal data processing is based on consent, individuals have the right to withdraw their consent at any time. Upon withdrawal of consent, National Medical Care Company, its branches, and its subsidiaries will stop processing the personal data for the relevant purpose unless another lawful basis for processing exists.

٩,٧ الحق في تقديم شكوى

يحق للأفراد الذين يعتقدون أن بياناتهم الشخصية قد تمت معالجتها بما يخالف متطلبات حماية البيانات المعمول بها تقديم شكوى إلى الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة.

9.7 Right to File a Complaint

Individuals who believe that their personal data has been processed in violation of applicable data protection requirements may submit a complaint to National Medical Care Company, its branches, and its subsidiaries.

National Medical Care Company, its branches, and its subsidiaries will review and address such complaints in accordance with its internal procedures.

وتقوم الشركة بمراجعة هذه الشكاوى ومعالجتها وفقاً لإجراءاتها الداخلية المعتمدة.

If the individual is not satisfied with the outcome, they may escalate the matter to the competent supervisory authority, which is currently the Saudi Data and Artificial Intelligence Authority (SDAIA).

9.8 Right to Claim Compensation

Individuals may have the right to claim compensation for any material or moral damage resulting from a violation of the Personal Data Protection Law and its Implementing Regulations, in accordance with applicable legal provisions.

Exercising Rights

National Medical Care Company, its branches, and its subsidiaries has established Data Subject Request procedure to manage requests from individuals seeking to exercise their data protection rights. Requests will be reviewed and responded to within the timeframes required by applicable regulations.

Individuals may submit requests through the official communication channels designated by National Medical Care Company, its branches, and its subsidiaries for privacy and data protection matters. All requests will be handled in a secure and confidential manner to protect the identity and personal data of the requesting individual.

10. Security Measures to Protect Data

National Medical Care Company, its branches, and its subsidiaries is committed to protecting the confidentiality, integrity, and availability of personal data processed within its operations. The company implements appropriate technical and organizational security measures to safeguard personal data against unauthorized access, disclosure, alteration, loss, or destruction.

These measures are designed to ensure that personal data is protected throughout its lifecycle and that access to personal data is limited to authorized personnel who require such access to perform their duties. Security controls are regularly reviewed and updated to address emerging risks and evolving security threats.

وفي حال عدم رضا الفرد عن نتيجة معالجة الشكوى، يحق له تصعيد الأمر إلى الجهة الرقابية المختصة، وهي حاليًا الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا).

٩,٨ الحق في المطالبة بالتعويض

قد يحق للأفراد المطالبة بالتعويض عن أي ضرر مادي أو معنوي ناتج عن مخالفة نظام حماية البيانات الشخصية ولوائحه التنفيذية، وذلك وفقًا للأحكام النظامية المعمول بها.

ممارسة الحقوق

قامت الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة بوضع إجراءات مخصصة لطلبات أصحاب البيانات لإدارة الطلبات المقدمة من الأفراد الراغبين في ممارسة حقوقهم المتعلقة بحماية البيانات. ويتم مراجعة هذه الطلبات والرد عليها خلال المدد الزمنية المحددة في الأنظمة المعمول بها.

ويمكن للأفراد تقديم طلباتهم من خلال القنوات الرسمية المعتمدة لدى الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة والمتعلقة بشؤون الخصوصية وحماية البيانات. ويتم التعامل مع جميع الطلبات بطريقة آمنة وسرية لضمان حماية هوية وبيانات مقدم الطلب.

١٠. تدابير الأمن لحماية البيانات

تلتزم الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة بحماية سرية وسلامة وتوافر البيانات الشخصية التي تتم معالجتها ضمن عملياتها. وتطبق الشركة تدابير أمنية تقنية وتنظيمية مناسبة لحماية البيانات الشخصية من الوصول غير المصرح به، أو الإفصاح، أو التعديل، أو فقدان، أو الإلتلاف.

وقد تم تصميم هذه التدابير لضمان حماية البيانات الشخصية طوال دورة حياتها، ولحصر الوصول إليها على الأشخاص المخولين الذين تتطلب مهامهم ذلك. كما تتم مراجعة الضوابط الأمنية وتحديثها بشكل دوري لمواكبة المخاطر الناشئة والتطورات في التهديدات الأمنية.

10.1 Commitment to Data Protection

National Medical Care Company, its branches, and its subsidiaries recognizes that protecting personal data is a critical responsibility, particularly in a healthcare environment where sensitive personal data such as medical and health information is processed.

National Medical Care Company, its branches, and its subsidiaries is committed to implementing effective security controls and maintaining strong governance practices to ensure that personal data is handled responsibly and in accordance with the requirements of the Kingdom of Saudi Arabia Personal Data Protection Law (KSA PDPL) and other applicable regulatory obligations.

All employees and authorized personnel are required to comply with National Medical Care Company, its branches, and its subsidiaries security policies and procedures when accessing or processing personal data.

10.2 Technical Security Measures

National Medical Care Company, its branches, and its subsidiaries implements a range of technical safeguards to protect personal data processed within its systems and digital platforms. These measures include secure system configurations, encryption where appropriate, and monitoring mechanisms designed to detect and prevent unauthorized access.

Technical controls may include:

- Encryption of personal data during storage and transmission where required.
- Access control mechanisms to ensure that only authorized personnel can access personal data.
- Secure authentication procedures for system access.
- Monitoring of system activity and access logs to detect potential security incidents.
- Network security controls such as firewalls and intrusion detection mechanisms.
- Data Loss Prevention (DLP) policies and tools.

١٠,١ الالتزام بحماية البيانات

تدرك الشركة الوطنية للرعاية الطبية وفروعها والشركات التابعة لها أن حماية البيانات الشخصية تعد مسؤولية بالغة الأهمية، لا سيما في بيئة الرعاية الصحية التي يتم فيها معالجة بيانات شخصية حساسة مثل المعلومات الطبية والصحية.

وتلتزم الشركة الوطنية للرعاية الطبية وفروعها والشركات التابعة لها بتطبيق ضوابط أمنية فعالة والحفاظ على ممارسات حوكمة قوية لضمان التعامل مع البيانات الشخصية بمسؤولية ووفقاً لمتطلبات نظام حماية البيانات الشخصية في المملكة العربية السعودية وغيرها من الالتزامات التنظيمية المعمول بها.

كما يُطلب من جميع الموظفين والأشخاص المصرح لهم الالتزام بسياسات وإجراءات الأمن الخاصة بالشركة الوطنية للرعاية الطبية وفروعها والشركات التابعة لها عند الوصول إلى البيانات الشخصية أو معالجتها.

١٠,٢ التدابير الأمنية التقنية

تطبق الشركة مجموعة من الضوابط التقنية لحماية البيانات الشخصية داخل أنظمتها ومنصاتها الرقمية. وتشمل هذه التدابير إعدادات الأنظمة الآمنة، وتقنيات التشفير عند الحاجة، وآليات المراقبة المصممة لاكتشاف ومنع الوصول غير المصرح به.

وقد تشمل الضوابط التقنية ما يلي:

- تشفير البيانات الشخصية أثناء التخزين والنقل عند الحاجة.
- آليات التحكم في الوصول لضمان قصر الوصول على الأشخاص المخولين.
- إجراءات مصادقة آمنة للدخول إلى الأنظمة.
- مراقبة أنشطة النظام وسجلات الدخول لاكتشاف الحوادث الأمنية المحتملة.
- ضوابط أمن الشبكات مثل الجدران الحماية وآليات كشف التسلل.
- سياسات وأدوات منع فقدان البيانات

These measures help ensure that National Medical Care Company, its branches, and its subsidiaries systems remain secure and that personal data is protected against unauthorized access or misuse.

10.3 Organizational Security Measures

In addition to technical controls, National Medical Care Company, its branches, and its subsidiaries implements organizational measures to ensure that personal data is handled responsibly by employees and authorized personnel.

Organizational safeguards include clearly defined roles and responsibilities for data protection, confidentiality obligations for employees, and procedures governing access to personal data.

National Medical Care Company, its branches, and its subsidiaries also ensures that third parties processing personal data on its behalf are subject to appropriate contractual obligations requiring them to implement adequate security measures and comply with applicable data protection requirements.

Through these combined technical and organizational controls, National Medical Care Company, its branches, and its subsidiaries aims to maintain a secure environment that protects personal data and supports compliance with relevant data protection laws.

11. Data Sharing with Third Parties

National Medical Care Company, its branches, and its subsidiaries may share personal data with third parties when necessary to support healthcare services, operational activities, or to comply with legal and regulatory obligations. When sharing personal data, the Company ensures that appropriate safeguards are implemented to protect the confidentiality and security of the data.

وتساهم هذه التدابير في ضمان أمن أنظمة الشركة الوطنية للرعاية الطبية وفروعها وشركاتها التابعة، وحماية البيانات الشخصية من الوصول غير المصرح به أو إساءة الاستخدام.

١٠,٣ التدابير الأمنية التنظيمية

بالإضافة إلى الضوابط التقنية، تطبق الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة تدابير تنظيمية لضمان تعامل الموظفين والأشخاص المخولين مع البيانات الشخصية بمسؤولية.

وتشمل هذه الضوابط تحديد الأدوار والمسؤوليات بشكل واضح فيما يتعلق بحماية البيانات، وفرض التزامات السرية على الموظفين، ووضع إجراءات منظمة للتحكم في الوصول إلى البيانات الشخصية.

كما تضمن الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة أن الأطراف الثالثة التي تعالج البيانات الشخصية نيابة عنها تخضع لالتزامات تعاقدية مناسبة تلزمها بتطبيق تدابير أمنية كافية والامتثال لمتطلبات حماية البيانات المعمول بها.

بواسطة هذه الضوابط التقنية والتنظيمية المجمع، تهدف الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة إلى الحفاظ على بيئة آمنة تحمي البيانات الشخصية وتدعم الامتثال لأنظمة حماية البيانات ذات الصلة.

١١. مشاركة البيانات مع أطراف ثالثة

يجوز للشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة مشاركة البيانات الشخصية مع أطراف ثالثة عند الضرورة لدعم خدمات الرعاية الصحية، أو الأنشطة التشغيلية، أو للامتثال للالتزامات النظامية والتنظيمية. وعند مشاركة البيانات الشخصية، تضمن الشركة تطبيق الضوابط المناسبة لحماية سرية البيانات وأمنها.

All data sharing activities must comply with the Kingdom of Saudi Arabia Personal Data Protection Law (KSA PDPL) and its Implementing Regulations.

The company ensures that personal data is shared only for legitimate purposes and only to the extent necessary to fulfil the intended purpose.

11.1 Types of Third Parties

National Medical Care Company, its branches, and its subsidiaries may share personal data with carefully selected third parties that support its operations and service delivery. These third parties may include:

- Healthcare service providers and laboratories involved in patient care.
- Insurance providers and claims administrators responsible for processing insurance claims.
- IT service providers responsible for maintaining healthcare information systems and digital infrastructure.
- Professional advisors such as legal consultants, auditors, and compliance advisors.
- Government and regulatory authorities where disclosure is required by law.
- Vendors and contractors providing operational services to National Medical Care Company, its branches, and its subsidiaries.

11.2 Types of Data Shared

The type of personal data shared with third parties depends on the purpose of the data sharing and the services being provided. This may include personal identification details, contact information, medical information required for treatment or insurance processing, employment information related to workforce management, and operational data necessary for service delivery.

National Medical Care Company, its branches, and its subsidiaries ensures that only the minimum amount of personal data necessary to fulfil the intended purpose is shared with third parties.

ويجب أن تتوافق جميع أنشطة مشاركة البيانات مع نظام حماية البيانات الشخصية في المملكة العربية السعودية ولوائحه التنفيذية. كما تضمن الشركة أن تتم مشاركة البيانات فقط لأغراض مشروعة وبالحد الأدنى اللازم لتحقيق الغرض المطلوب.

١١,١ أنواع الأطراف الثالثة

قد تقوم الشركة الوطنية للرعاية الطبية وفروعها والشركات التابعة لها بمشاركة البيانات الشخصية مع أطراف ثالثة يتم اختيارها بعناية لدعم عملياتها وتقديم خدماتها. وقد تشمل هذه الأطراف ما يلي:

- مقدمو خدمات الرعاية الصحية والمختبرات المشاركون في رعاية المرضى.
- شركات التأمين والجهات المسؤولة عن إدارة مطالبات التأمين.
- مزودو خدمات تقنية المعلومات المسؤولون عن صيانة أنظمة المعلومات الصحية والبنية التحتية الرقمية.
- المستشارون المهنيون مثل المستشارين القانونيين، والمدققين، ومستشاري الامتثال.
- الجهات الحكومية والتنظيمية عندما يكون الإفصاح مطلوباً بموجب الأنظمة والقوانين.
- الموردون والمتعاقدون الذين يقدمون خدمات تشغيلية للشركة الوطنية للرعاية الطبية وفروعها والشركات التابعة لها.

١١,٢ أنواع البيانات التي تتم مشاركتها

يعتمد نوع البيانات الشخصية التي تتم مشاركتها مع الأطراف الثالثة على الغرض من المشاركة والخدمات المقدمة. وقد تشمل هذه البيانات معلومات التعريف الشخصية، وبيانات الاتصال، والمعلومات الطبية اللازمة للعلاج أو معالجة التأمين، ومعلومات التوظيف المتعلقة بإدارة الموارد البشرية، والبيانات التشغيلية الضرورية لتقديم الخدمات.

وتحرص الشركة الوطنية للرعاية الطبية وفروعها وشركاتها التابعة على مشاركة الحد الأدنى فقط من البيانات الشخصية اللازمة لتحقيق الغرض المحدد.

١١,٣ الغرض من مشاركة البيانات

قد تتم مشاركة البيانات الشخصية مع أطراف ثالثة لأغراض تشمل دعم العلاج والخدمات الصحية، ومعالجة مطالبات التأمين وأنشطة الفوترة، وإدارة الأنظمة والبنية التحتية التشغيلية، والوفاء بالالتزامات التعاقدية، والامتثال لمتطلبات التقارير النظامية أو التنظيمية.

كما قد تتم مشاركة البيانات لدعم الأنشطة التشغيلية مثل إدارة الموردين، وصيانة المرافق، والخدمات الاستشارية المهنية.

11.3 Purpose of Data Sharing

Personal data may be shared with third parties for purposes including supporting medical treatment and healthcare services, processing insurance claims and billing activities, maintaining information systems and operational infrastructure, fulfilling contractual obligations, and complying with legal or regulatory reporting requirements.

Data sharing may also occur to support operational activities such as vendor management, facility maintenance, and professional advisory services.

١١,٤ الضمانات التعاقدية

عند قيام أطراف ثالثة بمعالجة البيانات الشخصية نيابة عن الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة ، يتم وضع ضمانات تعاقدية مناسبة لضمان معالجة البيانات الشخصية بشكل آمن ووفقاً للأنظمة المعمول بها في مجال حماية البيانات.

وقد تشمل هذه الضمانات ما يلي:

- Data Processing Agreements (DPAs) that clearly define the responsibilities of the third party when processing personal data on behalf of National Medical Care Company, its branches, and its subsidiaries. These agreements ensure that the third party processes personal data only in accordance with the Company instructions and implements appropriate security measures.
- Non-Disclosure Agreements (NDAs) that require third parties to maintain the confidentiality of personal data and prevent unauthorized disclosure or misuse of the information.
- Contractual provisions that require third parties to implement appropriate technical and organizational security controls to protect personal data.

- اتفاقيات معالجة البيانات التي تحدد بوضوح مسؤوليات الطرف الثالث عند معالجة البيانات نيابة عن الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة ، وتضمن الالتزام بتعليمات الشركة وتطبيق التدابير الأمنية المناسبة
- اتفاقيات عدم الإفصاح التي تلزم الأطراف الثالثة بالحفاظ على سرية البيانات ومنع الإفصاح أو الاستخدام غير المصرح به
- بنود تعاقدية تلزم الأطراف الثالثة بتطبيق ضوابط تقنية وتنظيمية مناسبة لحماية البيانات الشخصية.

Through these contractual mechanisms, National Medical Care Company, its branches, and its subsidiaries ensures that third parties maintain

ومن خلال هذه الآليات التعاقدية، تضمن الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة التزام الأطراف الثالثة بمعايير كافية لحماية البيانات عند التعامل معها.

adequate data protection standards when handling personal data.

11.5 Cross-border Data Transfer

In certain situations, personal data may be transferred outside the Kingdom of Saudi Arabia when necessary to support healthcare services, operational requirements, or collaboration with external service providers.

Where cross-border transfers occur, National Medical Care Company, its branches, and its subsidiaries ensures that such transfers comply with the requirements of the KSA PDPL and that appropriate safeguards are implemented to protect personal data. These safeguards may include:

- Conducting assessments to ensure that the destination country provides an adequate level of data protection.
- Implementing Standard Contractual Clauses (SCCs) or equivalent contractual mechanisms to ensure that personal data remains protected when transferred to another jurisdiction.
- Ensuring that third parties receiving personal data outside the Kingdom implement appropriate security measures and comply with National Medical Care Company, its branches, and its subsidiaries data protection requirements.

National Medical Care Company, its branches, and its subsidiaries ensures that any cross-border transfer of personal data is conducted in a controlled and lawful manner while maintaining the privacy and security of individuals' personal data.

12. Data Breach Response

National Medical Care Company, its branches, and its subsidiaries is committed to responding promptly and effectively to any incident that may compromise the security of personal data.

The Company has established procedures to detect, assess, manage, and report personal data breaches in accordance with the Kingdom of Saudi Arabia Personal

١١,٥ نقل البيانات عبر الحدود

في بعض الحالات، قد يتم نقل البيانات الشخصية خارج المملكة العربية السعودية عند الضرورة لدعم خدمات الرعاية الصحية أو المتطلبات التشغيلية أو التعاون مع مقدمي الخدمات الخارجيين.

وعند حدوث عمليات نقل عبر الحدود، تضمن الشركة التزام هذه العمليات بمتطلبات نظام حماية البيانات الشخصية، وتطبيق الضوابط المناسبة لحماية البيانات. وقد تشمل هذه الضوابط:

- إجراء تقييمات للتأكد من أن الدولة المستقبلة توفر مستوى كافٍ من حماية البيانات.
- تطبيق الشروط التعاقدية القياسية أو آليات تعاقدية مكافئة لضمان استمرار حماية البيانات بعد نقلها.
- التأكد من التزام الأطراف المستقبلية للبيانات خارج المملكة بتطبيق تدابير أمنية مناسبة والامتثال لمتطلبات الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة

وتضمن الشركة الوطنية للرعاية الطبية وفروعها وشركاتها التابعة أن أي نقل للبيانات الشخصية عبر الحدود يتم بطريقة محكمة وقانونية، مع الحفاظ على خصوصية وأمن البيانات الشخصية للأفراد.

١٢. الاستجابة لاختراق البيانات

تلتزم الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة بالاستجابة السريعة والفعالة لأي حادث قد يؤثر على أمن البيانات الشخصية.

وقد وضعت الشركة إجراءات للتعرف على حوادث اختراق البيانات الشخصية وتقييمها وإدارتها والإبلاغ عنها وفقاً لنظام حماية البيانات الشخصية في المملكة العربية السعودية ولوائح

Data Protection Law (KSA PDPL) and its Implementing Regulations.

These procedures are designed to minimize potential harm to individuals, ensure regulatory compliance, and strengthen security controls to prevent future incidents.

12.1 Personal Data Breach

A Personal Data Breach, as defined in Chapter 3 of this policy, refers to any security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data processed by National Medical Care Company, its branches, and its subsidiaries.

Such incidents may arise from system vulnerabilities, human error, malicious activities, or technical failures. Any event that compromises the confidentiality, integrity, or availability of personal data must be treated as a potential data breach and handled in accordance with National Medical Care Company, its branches, and its subsidiaries incident response procedures.

12.2 Response Procedures

When a potential personal data breach is identified, National Medical Care Company, its branches, and its subsidiaries will take immediate steps to assess and contain the incident. The objective of the response process is to prevent further unauthorized access, minimize potential damage, and protect affected personal data.

Initial response actions may include:

- Securing or isolating affected systems.
- Preventing further unauthorized access to personal data.
- Assessing the nature and scope of the breach.
- Identifying the categories of personal data affected.
- Determining the potential impact on

التنفيذية.

وتهدف هذه الإجراءات إلى تقليل الأضرار المحتملة على الأفراد، وضمان الامتثال التنظيمي، وتعزيز الضوابط الأمنية لمنع تكرار الحوادث مستقبلاً.

١٢,١ اختراق البيانات الشخصية

يُقصد باختراق البيانات الشخصية، وفقاً للتعريف الوارد في الفصل الثالث من هذه السياسة، أي حادث أمني يؤدي إلى الإضرار العرضي أو غير النظامي، أو الفقد، أو التعديل، أو الإفصاح غير المصرح به، أو الوصول غير المصرح به إلى البيانات الشخصية التي تعالجها الشركة الوطنية للرعاية الطبية وفروعها وشركاتها التابعة.

وقد تنشأ هذه الحوادث نتيجة ثغرات في الأنظمة، أو أخطاء بشرية، أو أنشطة خبيثة، أو أعطال تقنية. ويجب التعامل مع أي حدث قد يؤثر على سرية أو سلامة أو توافر البيانات الشخصية باعتباره احتمالاً لاختراق بيانات ومعالجته وفقاً لإجراءات الاستجابة للحوادث لدى شركة رعاية الطبية الوطنية وفروعها وشركاتها التابعة.

١٢,٢ إجراءات الاستجابة

عند تحديد احتمال وقوع اختراق للبيانات الشخصية، تتخذ الشركة الوطنية للرعاية الطبية وفروعها وشركاتها التابعة خطوات فورية لتقييم الحادث واحتوائه. ويهدف هذا الإجراء إلى منع أي وصول غير مصرح به إضافي، وتقليل الأضرار المحتملة، وحماية البيانات المتأثرة.

وقد تشمل الإجراءات الأولية ما يلي:

- تأمين أو عزل الأنظمة المتأثرة.
- منع أي وصول غير مصرح به إضافي إلى البيانات الشخصية.
- تقييم طبيعة ونطاق الاختراق.
- تحديد فئات البيانات الشخصية المتأثرة.
- تحديد الأثر المحتمل على الأفراد.

individuals.

National Medical Care Company, its branches, and its subsidiaries will activate its internal incident management procedures to ensure that the breach is investigated and managed by the appropriate personnel.

وتقوم الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة بتفعيل إجراءات إدارة الحوادث الداخلية لضمان التعامل مع الحادث من قبل الجهات المختصة.

12.3 Investigation and Remediation

Following identification of a personal data breach, the Company will conduct a thorough investigation to determine the root cause of the incident and evaluate its impact.

The Data Protection Officer (DPO) will coordinate with relevant departments such as IT, Information Security, Legal, and Compliance to assess the incident and determine the appropriate response measures.

The investigation will evaluate:

- The cause and circumstances of the breach.
- The categories and volume of personal data involved.
- The potential risks to affected individuals.

Based on the findings, National Medical Care Company, its branches, and its subsidiaries will implement corrective measures to address the issue and strengthen existing security controls.

These actions may include improving system security, updating procedures, or providing additional training to employees.

١٢,٣ التحقيق والمعالجة

بعد تحديد وقوع اختراق للبيانات الشخصية، تقوم الشركة بإجراء تحقيق شامل لتحديد السبب الجذري للحادث وتقييم أثره.

ويتولى مسؤول حماية البيانات التنسيق مع الإدارات ذات العلاقة مثل تقنية المعلومات، وأمن المعلومات، والشؤون القانونية، والامتثال، لتقييم الحادث وتحديد الإجراءات المناسبة لمعالجته.

ويتم خلال التحقيق تقييم ما يلي:

- طبيعة وظروف اختراق البيانات.
- فئات وحجم البيانات الشخصية المتأثرة.
- المخاطر المحتملة على الأفراد المتأثرين.

وبناءً على النتائج، ستقوم الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة بتنفيذ إجراءات تصحيحية لمعالجة المشكلة وتعزيز الضوابط الأمنية القائمة.

وقد تشمل هذه الإجراءات تحسين أمن الأنظمة، أو تحديث الإجراءات، أو تقديم تدريب إضافي للموظفين.

12.4 Notification to Affected Individuals

If a personal data breach is likely to result in harm or significant risk to the rights or interests of individuals, the company will notify the affected individuals without undue delay.

The notification will provide clear and transparent information regarding:

- The nature of the personal data breach.

١٢,٤ إخطار الأفراد المتأثرين

في حال كان من المحتمل أن يؤدي اختراق البيانات الشخصية إلى ضرر أو مخاطر كبيرة على حقوق أو مصالح الأفراد، تقوم الشركة بإخطار الأفراد المتأثرين دون تأخير غير مبرر. ويتضمن الإخطار معلومات واضحة وشفافة بشأن:

- طبيعة اختراق البيانات الشخصية.
- الآثار المحتملة للاختراق.
- التدابير التي اتخذتها الشركة أو التي تعتزم اتخاذها لمعالجة

Data Protection and Privacy Policy

- The potential consequences of the breach.
- The measures taken or proposed by the Company to address the breach.
- Guidance on any actions individuals may take to mitigate potential risks.

Notifications will be communicated in a clear and understandable manner.

12.5 Reporting a Breach

All employees, contractors, and authorized personnel must immediately report any suspected or confirmed personal data breach through National Medical Care Company, its branches, and its subsidiaries designated internal reporting channels.

Where required under applicable regulations, the company will report personal data breaches to the competent regulatory authority, currently the Saudi Data and Artificial Intelligence Authority (SDAIA), in accordance with the requirements of the KSA PDPL.

Timely reporting and coordinated response are essential to ensure that personal data remains protected and that appropriate actions are taken to address any security incidents.

13. Employee Training

National Medical Care Company, its branches, and its subsidiaries recognizes that employee awareness and responsibility are essential to protecting personal data. As part of its commitment to compliance with the Kingdom of Saudi Arabia Personal Data Protection Law (KSA PDPL), the company ensures that employees understand their responsibilities when handling personal data and are aware of the importance of maintaining confidentiality and security.

The company provides data protection and privacy training to employees who process or have access to personal data as part of their roles. These training programs aim to ensure that employees understand applicable data protection requirements, internal policies, and the procedures they must follow when

الاختراق.

- الإرشادات المتعلقة بالإجراءات التي يمكن للأفراد اتخاذها لتقليل المخاطر المحتملة. وتتم عملية الإخطار بطريقة واضحة وسهلة الفهم.

١٢,٥ الإبلاغ عن الاختراق

يجب على جميع الموظفين والمقاولين والأشخاص المخولين بالإبلاغ الفوري عن أي اختراق بيانات شخصية مشتببه به أو مؤكد من خلال قنوات الإبلاغ الداخلية المعتمدة لدى الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة.

وعند الحاجة وفقاً للأنظمة المعمول بها، تقوم الشركة بالإبلاغ عن حالات اختراق البيانات الشخصية إلى الجهة الرقابية المختصة، وهي حالياً الهيئة السعودية للبيانات والذكاء الاصطناعي (سداء)، وذلك وفقاً لمتطلبات نظام حماية البيانات الشخصية.

ويُعد الإبلاغ في الوقت المناسب والتنسيق الفعال أمراً ضرورياً لضمان حماية البيانات الشخصية واتخاذ الإجراءات المناسبة لمعالجة أي حوادث أمنية.

١٣. تدريب الموظفين

تدرك الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة أن وعي الموظفين ومسؤوليتهم يُعدان عنصرين أساسيين في حماية البيانات الشخصية. وكجزء من التزامها بالامتثال لنظام حماية البيانات الشخصية في المملكة العربية السعودية، تضمن الشركة أن يكون الموظفون على دراية بمسؤولياتهم عند التعامل مع البيانات الشخصية، وبأهمية الحفاظ على سريتها وأمنها.

وتوفر الشركة برامج تدريبية في مجال حماية البيانات والخصوصية للموظفين الذين يتعاملون مع البيانات الشخصية أو لديهم صلاحية الوصول إليها ضمن مهامهم الوظيفية. وتهدف هذه البرامج إلى ضمان فهم الموظفين لمتطلبات حماية البيانات المعمول بها، والسياسات الداخلية، والإجراءات الواجب اتباعها عند جمع البيانات الشخصية أو استخدامها أو تخزينها أو مشاركتها.

collecting, using, storing, or sharing personal data.

Training may cover topics such as:

- Basic principles of personal data protection.
- Responsibilities of employees when handling personal data.
- Proper use of the company information systems and data access controls.
- Identification and reporting of personal data breaches or security incidents.
- Protection of sensitive personal data, including patient health information.

National Medical Care Company, its branches, and its subsidiaries may provide general data protection awareness training to all employees and additional role-specific training to personnel who regularly handle sensitive personal data or are responsible for managing data protection processes.

The Data Protection Officer (DPO) or the designated data protection function within the company may support the development and delivery of training programs to ensure that employees remain informed about data protection requirements and best practices.

14. Changes to Policy

National Medical Care Company, its branches, and its subsidiaries reserves the right to update or amend this Internal Data Protection and Privacy Policy when necessary to reflect changes in legal requirements, regulatory guidance, operational practices, or technological developments.

Updates to this policy may occur in response to changes in the Kingdom of Saudi Arabia Personal Data Protection Law (KSA PDPL), its Implementing Regulations, guidance issued by the Saudi Data and Artificial Intelligence Authority (SDAIA), or other applicable healthcare and regulatory requirements.

The company will review this policy periodically to ensure that it remains accurate, effective, and aligned with applicable laws and best practices in data protection and privacy management.

وقد تغطي برامج التدريب موضوعات مثل:

- المبادئ الأساسية لحماية البيانات الشخصية.
- مسؤوليات الموظفين عند التعامل مع البيانات الشخصية.
- الاستخدام الصحيح لأنظمة الشركة وضوابط الوصول إلى البيانات.
- التعرف على حوادث اختراق البيانات والإبلاغ عنها.
- حماية البيانات الشخصية الحساسة، بما في ذلك المعلومات الصحية للمرضى.

وقد تقدم الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة تدريباً عاماً للتوعية بحماية البيانات لجميع الموظفين، بالإضافة إلى تدريب متخصص مرتبط بطبيعة العمل للموظفين الذين يتعاملون بشكل متكرر مع بيانات حساسة أو المسؤولين عن عمليات إدارة حماية البيانات.

وقد يقوم مسؤول حماية البيانات أو الجهة المختصة بحماية البيانات داخل الشركة بدعم تطوير وتنفيذ برامج التدريب لضمان استمرار اطلاع الموظفين على متطلبات حماية البيانات وأفضل الممارسات.

١٤. التعديلات على السياسة

تحتفظ الشركة الوطنية للرعاية الطبية و فروعها و شركاتها التابعة بالحق في تحديث أو تعديل سياسة حماية البيانات والخصوصية الداخلية عند الحاجة، وذلك بما يعكس التغيرات في المتطلبات النظامية، أو التوجيهات التنظيمية، أو الممارسات التشغيلية، أو التطورات التقنية.

وقد يتم تحديث هذه السياسة استجابة للتغيرات في نظام حماية البيانات الشخصية في المملكة العربية السعودية ولوائحه التنفيذية، أو التوجيهات الصادرة عن الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا)، أو أي متطلبات تنظيمية أو صحية أخرى ذات صلة.

وتقوم الشركة بمراجعة هذه السياسة بشكل دوري لضمان بقائها دقيقة وفعالة ومتوافقة مع الأنظمة المعمول بها وأفضل ممارسات حماية البيانات والخصوصية.

Where significant changes are made to the policy, the company will communicate the updates to relevant employees and stakeholders through appropriate internal communication channels. Employees are expected to familiarize themselves with the updated policy and comply with its requirements when handling personal data.

The Data Protection Officer (DPO) or the designated data protection function within the company may oversee the review and update process to ensure that the policy continues to support the company data protection framework and regulatory compliance obligations.

وفي حال إجراء تغييرات جوهرية على السياسة، ستقوم الشركة بإبلاغ الموظفين والجهات ذات العلاقة من خلال قنوات الاتصال الداخلية المناسبة. ويُتوقع من الموظفين الاطلاع على النسخة المحدثة من السياسة والالتزام بمتطلباتها عند التعامل مع البيانات الشخصية.

وقد يتولى مسؤول حماية البيانات أو الجهة المختصة بحماية البيانات داخل الشركة الإشراف على عملية المراجعة والتحديث لضمان استمرار توافق السياسة مع إطار حماية البيانات والالتزامات التنظيمية للشركة.



Care Medical
Data Governance Committee
datagovern@care.med.sa