TITLE	**Data Classification and Labelling Standard**
TARGET AUDIENCE	Subject to any exceptions below, this Standard applies to all Cabrini's employees, contractors, and third-party service providers (henceforth all of them referred to as "personnel") responsible for creating, accessing, using, storing, processing, or transferring Cabrini's data.
SCOPE	This Standard applies to all data that is owned, stored and/or used by Cabrini and/or contained in any DNS domain owned by Cabrini. It is applicable to data hosted on Cabrini's premises and at external/third-party service providers if the data resides in a Cabrini domain or is owned by Cabrini.

PURPOSE

To ensure data protection is the foundation of trustworthy, safe patient care, business relationships and the reputation of Cabrini.

The Data Classification and Labelling Standard provides the framework for appropriate levels of data protection and handling for Cabrini to be compliant to regulations. This Policy is consistent with existing Cabrini IT policies as well as supporting Cabrini security procedures and standards.

- The primary purpose of this document is to ensure patient information is private and safe and is not compromised in capturing, storing, accessing, using, processing, or disposing of data.
- Establishing a Data Classification and Labelling Standard and the controls appropriate for each classification level is essential for protecting data throughout its lifecycle.
- Formalising data and labelling classification and protection requirements also enables Cabrini to meet its legal obligation to manage personal data.
- This document articulates Cabrini's Data Classification and Labelling Standard for data assets and the controls that should be implemented at each classification level.
- The appropriate data classification level is determined by the Business Owner, in consultation with the Privacy Officer if required, and reflects the value and sensitivity of the data and the impact to Cabrini if the data is compromised.
- A compromise of data is any loss in the confidentiality, integrity, or availability of that data.

DEFINITIONS

Cabrini	Cabrini Australia Limited and its subsidiaries.
Chief Information Officer	The executive in charge of information technology initiatives and strategy.
Client	(Legal and natural persons) are the existing or potential clients of Cabrini including the patients and their carers, employees, managers, general managers, or agents of legal entities for the existing or potential clients of Cabrini.

Criticality	A measure of the degree to which an organization depends on the data for the success of a mission or of a business function.
Data	Facts or figures, or information that is stored in physical or electronic mediums.
Business Owner	Person responsible for the business use of the data asset. This person will be in a senior role that has authority to determine the business use of the data asset.
Technical Owner	Individuals who control data assets and data systems regardless of physical or logical location, storage medium, technology used, format, or the purpose(s) they serve. The Technical Owner will be part of the IT Team, unless the Chief Information Officer (CIO), has confirmed there is business operational reason for specific data assets and data systems to be controlled by an individual outside of this team.
Data User	Individuals who have been granted explicit authorisation by the relevant Business Owner to create, access, use, alter, or destroy data within a data system.
Privacy Officer	Person who acts as the adjudicator with regards to the application of the Data Classification and Labelling standard.
Personal Information	Personal information can include a broad range of information, or an opinion, that could identify an individual. This may include but not limited to; name, signature, address, date of birth, medical information, photograph etc.
Information Technology	Team responsible for Cabrini information technology assets.
Sensitivity	Measure of the amount of harm that could result to Cabrini, Cabrini patients and/or third parties in the event of a compromise of the data.
Confidential Personal Information	Confidential information is personal information that includes but not limited to information or an opinion about an individual's racial or ethnic origin, sexual orientation or practices, criminal record or health information.
Third Party	Any individual or organisation not directly employed by Cabrini. Examples may include: Third Party service providers, cloud service providers, vendors, and contingent staff such as contractors, consultants, temporary workers, and vendors.
Unstructured Data	Unstructured data (or unstructured information) refers to information that either does not have a pre-defined data model or is not organised in a pre-defined manner. Unstructured information is typically text-heavy, but may contain data such as dates, numbers, such as COVID sign-in sheets.

APPLICATION OF STANDARD

This Standard does not apply to CTG Data to the extent that the Standard conflicts with CTG Data Governance and CTG Data Classification Procedure.

PRINCIPLES

The handling and classification of data within Cabrini must at all times be consistent with the highest level of protection for the privacy and security of patient data.

- Employees and contractors must be aware of the classification standards and procedures.
- The classification levels must be consistent across the whole organisation.
- Business Owners will only provide access to Data Users who have a legitimate need to access that information to fulfil their official duties or contractual responsibilities.
- If data is not classified by the Business Owner, it can be classified by the Technical Owner. If neither have classified the data, the default level of "confidential" will apply.
- It is the responsibility of Data Users granted access to ensure that the data is handled with due care and protected according to its security classification.

Backups

- Backup copies of important information, software and systems shall be taken at frequent intervals.
- Backup media shall be stored in a manner sufficient to escape any damage from a disaster at the main site.
- Backup media shall be regularly tested to ensure that it can be relied upon for emergency use when necessary; this shall be combined with a test of the restoration procedures and checked against the required restoration time.
- Proper data handling procedures shall be followed when transporting backup media, in line with data classifications.
- Software backups shall not be stored for longer than the recommended shelf lives of the storage media or beyond established retention periods.

Removable Media

- All highly sensitive and sensitive data stored on removable media shall be encrypted at rest.
- Removable media containing highly sensitive, sensitive, and confidential data shall be physically secured.
- Removable media containing highly sensitive, sensitive, and confidential data shall be transported by secured courier or other secure and trackable delivery mechanism.
- Removable media containing highly sensitive and sensitive data should be clearly labelled and accounted for in a managed and secure manner.

DATA CLASSIFICATION LEVELS

The Data Classification levels are:

	Description
Public	Data that is freely accessible to the public. It can be freely used, reused, and redistributed without repercussions. For example: staff directory data, marketing, and service data, published research data.
Confidential	Data that is accessible to internal Cabrini personnel or vendors who are granted access to perform a task. For example: business unit process and procedure, unpublished intellectual property, IT system design and configuration data, Intranet. ***Confidential*** *is the default data classification if no other classification level is assigned.*
Sensitive	Data that requires specific authorization and/or clearance. For example: staff HR data, patient non-medical data, organisational financial data, research data (containing personal data).
Highly Sensitive	Data that, if compromised or accessed without authorization, could lead to criminal charges and legal fines or cause irreparable damage to the company or seriously impact the health and safety of Cabrini patients. For example: data subject to regulatory control, employee relations and complaints data, patient medical data, credit card data; research data (containing personal medical data).

DATA CLASSIFICATION REQUIREMENTS

1. Data is to be classified using the Cabrini's Data Classification and Labelling Standard, which is described in Table 1.
2. The maximum applicable classification level from Table 1 should be applied.
3. Data is to be classified in terms of legal requirements, sensitivity, criticality, and risk to Cabrini.
4. Data in aggregate should be classified one up, ie: the classification level should be increased for when information assets at lower classification levels are grouped together. This is because of the potential for increased impact when different types of information can be correlated.
5. If data is to be retained via physical or electronic storage mediums, including retention within Information Technology Assets, it is to be classified upon its creation by the Business Owner.
6. Information storage mediums should be classified to the highest level of the data it stores.
7. Confidential is the default data classification if no other classification level is assigned.
8. Data is to be re-classified by the Business Owner upon significant change in legal requirements, sensitivity, criticality, or risk to the Cabrini.
9. Data should only be stored, processed, and communicated on system(s) designed to support the classification level and appropriate management of that data.

Table 1 – Data Classification and Labelling Standard

	SEVERITY			
IMPACT TYPE	**Lowest**	<------>		**Highest**
Impact	**Negligible to Minor**	**Moderate**	**Major**	**Severe**
What advantage does this data provide to malicious persons	Little or no advantage.	Might provide some advantage.	Definite advantage.	Significant advantage.
Likelihood of malicious persons searching for this data.	Rare or unlikely	Possible	Likely	Almost certain
Consequences if this data is disclosed, stolen or lost. per Cabrini ERM Framework Measures of Consequence (Organisation Level)				

IMPACT TYPE	SEVERITY			
	Lowest	<------>		Highest
Impact	**Negligible to Minor**	**Moderate**	**Major**	**Severe**
Safety (clients, patients)	Patient suffers mild discomfort at disclosure. *Not applicable for data classification. Lowest classification level for client / patient data is "Confidential".*	Patient may discontinue ongoing treatment.	Patient employment or reputation may be compromised.	Patient life or safety placed in danger – from either themselves or others.
Mission, Identity, ethics & values	None to minor effect on ethical standards; holistic patient care; Cabrini Mission and values; services to the community	Evidence or some decline in ethical standards; holistic patient care; Cabrini Mission and values; services to the community	Measurable and major decline in ethical standards, holistic patient care; Cabrini Mission and values; services to the community	Ongoing or prolonged breach(es) or sustained degradation of ethical standards; holistic patient care, Cabrini Mission and values; services to the community
Reputation	None to mild damage to reputation; and / or Low impact, low news profile	Loss of reputation affecting propensity to offer additional services; and / or Moderate impact,	Extreme influence on Cabrini reputation resulting in major loss of patients and referrals; and / or High impact and high news profile	Damage to Cabrini reputation resulting in profound loss of patients and referrals; and / or Very high impact, high widespread multiple media coverage
Financial / Commercial / Compliance	Financial impact of <1% - 5% of budgeted annual EBITDA; Basic, supervisory and / or monitoring controls are operating as effectively and / or as intended, recommendation for improvements to strengthen control, a process improvement opportunity; Full accreditation / license / certification granted with recommendations requiring none or some additional resources	Financial impact of 5% - 10% of budgeted annual EBITDA; Basic, supervisory and / or monitoring controls are partly inadequate and require attention; High priority recommendations from accrediting / licensing / certifying body requiring timely action to maintain accreditation / certification	Financial impact of 10% - 25% of budgeted annual EBITDA; Basic, supervisory and / or monitoring controls are inadequate and require prompt attention; Loss of accreditation / license / certification resulting in sanctions imposed by the accrediting / certifying body	Financial impact of >/= 25% of budgeted annual EBITDA; Basic, supervisory and/or monitoring controls are inadequate and require immediate attention; Loss of accreditation / license / certification resulting in closure of the facility or significant reduction in service
Safety (employees)	None to minor injuries to an employee(s)	Series of treatable injuries to an employee(s)	Serious injuries to an employee(s)	Death and / or serious permanent injury of an employee
Example data types	Staff directory data. Marketing and Service data; Published research data.	Business unit process and procedure; Unpublished intellectual property; IT system design and configuration data; Intranet.	Staff HR Data; Patient non-medical data; Organisational financial data; Research Data (containing personal data).	Data subject to regulatory control; Employee relations and complaints data; Patient medical data. Credit card data; Research data (containing personal medical data).
Recommended data Sensitivity classification	**Public**	**Confidential**	**Sensitive**	**Highly Sensitive**

The recommended Data Sensitivity classification table above (Table 1) is to be used as an indication of the Data Protection Requirements that are applied throughout the data lifecycle.

If the functionality available within a process and / or Information Technology asset enables the application of the data protection requirements at different levels of protection, the Data Sensitivity classification should be assigned at the highest assignable level to meet the data protection requirements for the data at each classification level.

If the functionality available within a process and / or Information Technology asset does not enable the application of the data protection requirements at different levels of protection, the highest data Sensitivity classification assignable to the data applies for determining the data protection requirements.

DATA PROTECTION REQUIREMENTS

Data protections are defined for each Sensitivity classification level and must be applied throughout the data lifecycle. The protections address data confidentiality, integrity, and availability requirements and are described in Table 2.

Table 2 - Data Protections

Control Category	Description of Controls	Public	Confidential	Sensitive	Highly Sensitive
Access Control	No restriction on viewing	X			
	Role-based access to IT resources and data		X	X	X
	Access to authorised users only		X	X	X
	Authentication and authorisation required for access		X	X	X
	Business Owner must grant permission for access			X	X
	Authorisation by Business Owner required for modification	X	X	X	X
	Non-disclosure agreement required to be signed by third parties if not covered by a third party MSA		X	X	X
	Accounts with elevated access to data (Administration, Privileged etc.) must have complex credentials configured.		X	X	X
Copying / Printing (paper and electronic forms)	No restrictions	X			
	Should not be left unattended on a physically insecure printer		X	X	X
	Data should only be printed when there is a legitimate need		X	X	X
	Electronic and physical copies must be labelled according to their data classification. Any unlabelled data will be assumed to have the "confidential" classification by default.		X	X	X
	Copies must be limited to Data Users		X	X	X

Table 2 - Data Protections					
Control Category	**Description of Controls**	**Public**	**Confidential**	**Sensitive**	**Highly Sensitive**
Network Security	Protection with firewall and Intrusion Prevent System (IPS) required	X	X	X	X
	Access to user interfaces must be via a virtual server or reverse proxy. No direct access to servers permitted for end users	X	X	X	X
	Servers hosting the data should not be visible to the Internet. Presentation layer services should reside in a DMZ network		X	X	X
	Servers hosting the data should not be visible to unprotected internal networks such as Guest		X	X	X
	Transmission of personally identifiable data should be de-identified / anonymised when transmitted externally			X	X
System Security	Systems should be hardened as per vendor hardening guidelines and applicable internal hardening standards	X	X	X	X
	Apply security patches within defined SLA	X	X	X	X
	Endpoint protection software must be installed on all applicable systems, and must be automatically updated with the latest signatures	X	X	X	X
	Host-based firewall enabled in default deny mode, and permit minimum necessary services			X	X
	System storage must be encrypted			X	X
	Data should not be stored or processed on portable devices and removable media. Data should remain secured within the Cabrini Data Centre environment and encrypted-at-rest.			X	X
	Production (actual) data should not be used in test or development environments without being de-identified or obfuscated		X	X	X
Physical Security	Facility that provides access to data must be locked or logged out when unattended or unused		X	X	X
	Documents and data assets to be stored in approved and supported environments		X	X	X
	Must be hosted in a Secure Data Centre			X	X
	Physical access must be monitored, logged, and limited to Data Users			X	X
	Requires user authentication	X	X	X	X

Table 2 - Data Protections					
Control Category	**Description of Controls**	**Public**	**Confidential**	**Sensitive**	**Highly Sensitive**
Remote Access to systems hosting data for administrative purposes	Multi-Factor Authentication recommended for roles with administrative access to data	X	X	X	X
	Multi-Factor Authentication required for roles with administrative access to data		X	X	X
	Access to administrative interfaces restricted to IT Management networks, or via a Jump Server, or protected with Multi-Factor Authentication		X	X	X
	Remote access by third party for technical support limited to authenticated VPN, or via supervised session utilising MS Teams or similar		X	X	X
	Unsupervised remote access by third party, such as an application vendor, for technical support is not allowed, unless covered by an appropriate formal agreement stipulating data handling requirements equivalent to or stronger than those in this document		X	X	X
Audit logs	Logging of login and logoff events, and login failures		X	X	X
	Logging of delete events			X	X
	Forward logs to a remote log management server (SIEM)			X	X
	Logging of read and write events			X	X
Encryption of data in transit	Encryption required (e.g. HTTPS, SCP, SFTP)	X	X	X	X
	Must not be sent directly via standard, unencrypted email			X	X
Encryption of data at rest	Data must be kept encrypted while stored on disk.			X	X
Backups	Daily backups required	X	X	X	X
	Geographically dispersed storage required			X	X
Disposal	All disposals of data (electronic and hard copy) must be made in accordance with the appropriate Cabrini Record Retention and Disposal policy	X	X	X	X
	Paper-based data shredded and placed in managed confidential bins		X	X	X
	Wipe, erase or destroy electronic media such as hard drives, USBs, CD and DVDs		X	X	X

ALIGNMENT WITH GOVERNMENT SECURITY CLASSIFICATION

The Data Classification and Labelling Standard broadly aligns with the VIC and Commonwealth information classification schemes.

Cabrini	VIC	Commonwealth
Public	UNOFFICIAL and OFFICIAL	UNOFFICIAL and OFFICIAL
Confidential	OFFICIAL: Confidential	OFFICIAL: Confidential
Sensitive	PROTECTED	PROTECTED
Highly Sensitive	SECRET	SECRET
N/A	TOP SECRET	TOP SECRET

The VIC and Commonwealth classifications and associated protections must be applied when dealing with state and federal government information. In these scenarios, guidance on implementing data protections must be sought from the Business Owner and Privacy Officer.

ROLES AND RESPONSIBILITIES

Roles	Responsibility
Chief Information Officer	The Chief Information Officer is responsible for the implementation and enforcement of this Standard.
Privacy Officer	The Privacy Officer serves as a point of escalation for governance, data quality issues and will work closely with Business Owners and Functional area leadership to improve the quality and value of core data assets, respond to regulatory protection requirements as well as support the strategic requirements of the department. The Privacy Officer may take or delegate the role for leading enterprise privacy and data protection. The Privacy Officer contributes to the data protection strategy and implementation to ensure compliance with regulation. Responsibilities include: • managing interdependencies between the data governance group and other internal groups, • identifying/resolving/escalating issues, • achieving objectives within the scope of data governance, • providing the necessary data governance knowledge capital to Cabrini • managing overall establishment, implementation, maintenance, and continual improvement of the Data Governance Program, • reviewing compliance with data governance standards across Cabrini, and • updating the data governance policies whenever necessary, • notifying and otherwise communicating information about personal data breaches, and • documenting public and regulators' requests regarding the removal, destruction, and accessibility of data.
Business Owner	The Business Owner serves as the data authority for their business area. They serve as the owner of the data created and handled by their line of business. Business Owners are the decision makers for establishing data quality requirements and for overseeing and implementing the necessary safeguards to protect data. Responsibilities include: • ensuring data quality through fit-for-purpose requirements • identifying and prioritizing key systems or processes for improvement, • ensuring data management procedures and processes within their business area are documented, • prioritizing data and data management requirements, • ensuring data management issues are resolved in a timely manner, • ensuring data and data management functions are monitored and improved, • authorizing user access to data assets within their business area in consultation with the Technical Owner, and • ensuring staff are trained and competent to fulfil their data management duties, • owning the implementation and ongoing management of data quality improvements, • establishing data quality requirements (timeliness, accuracy, completeness, accessibility), • determining and approving access and re-use of data, • establishing the backup/recovery/archiving requirements, • understanding legal/compliance/regulatory issues impacting data, • setting priorities and sponsoring projects for all work related to the maintenance and processing of the data, • approving all governance matters impacting the processing of data, and • ensuring data security, backup, and archiving requirements are being met.
Technical Owner	Technical Owners are responsible for the technical control of data including security, scalability, configuration management, availability, accuracy, consistency, audit trail, backup and restore, technical standards, policies and business rule implementation. The functions of the Technical Owner are: • data compliance at a technical level, • data storage and security at a technical level, • data standards and quality at a technical level, and • data access (use and disclosure) at a technical level.
Data User	Every person who is an authorized user of a data asset is responsible for: • ensuring their access to data is carried out in a way which does not jeopardize data security and privacy, • not allowing their usernames or passwords to be used by any other person or accessing data on behalf of any other person. Any person wishing to access data should seek approval from the Business Owner and apply for authorisation to the Technical Owner, • ensuring that paper documents with personal or confidential information are stored securely and are not viewable by others during use, • reporting any breach or suspected breach of data security or privacy to the Data Protection Officer, • striving to ensure that data is complete, accurate and up to date, and • complying with relevant policies and procedures.
All Personnel	All personnel (including staff and contractors) are responsible for: • complying with applicable data governance policies and regulations • participating in training related to data governance, and • remaining aware of their data governance roles, responsibilities, and obligations.

REVIEW

This policy is to be reviewed at least every two years or at any time there are significant changes to the regulatory and threat landscape or business objectives. This is to ensure the policy remains aligned with business requirements, applicable legislation, standards, and information security best practices.

On review, the policy will be presented to the Group Executive for endorsement.

REFERENCES and ASSOCIATED DOCUMENTS

Cabrini Policies Procedures and Protocols

Information Security Policy
Acceptable Usage Policy
Access Control Policy
Cryptographic Controls Policy
Cyber Security Incident Response Policy
Cyber Security Risk Management Policy
Electronic Communication Policy
IT Asset Management Policy
IT Change Management Policy
Logging and Monitoring Policy
Mobile Device and Teleworking Policy
Third Party Security Policy
Cyber Security Risk Management Process
Vulnerability Management Process
Privacy Management Process
Enterprise Risk Management Framework
Cabrini Research Data Governance Checklist

Key Legislation and Standards

Health Records Act 2001 (Vic)
Public Records Act 1973 (Vic)
Victorian Protective Data Security Standards
Protective Security Policy Framework
ISO/ISE 27001:2013 Information Security Management System
ISO/ISE 27001:2022 Information Security Management System
Information Security Manual

References

https://www.nist.gov/cyberframework
https://www.cisecurity.org/controls/cis-controls-list
https://ovic.vic.gov.au/resource/victorian-protective-data-security-standards
https://www.protectivesecurity.gov.au
https://www.cyber.gov.au/acsc/view-all-content/ism

REVISION HISTORY

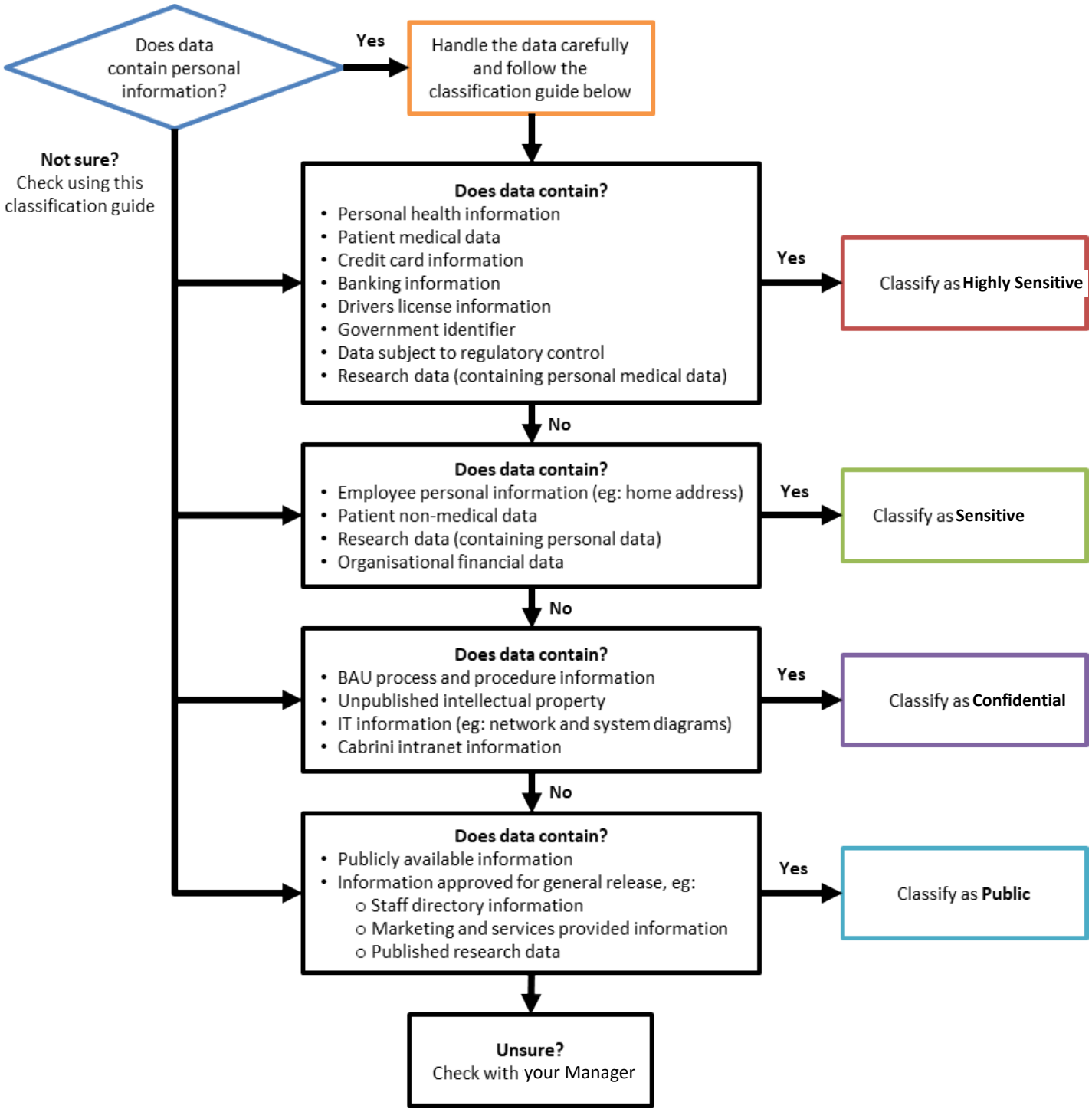
Version	Revision date	Revision notes
V0.1	24/1/23	Initial draft
V0.2	15/1/23	Updated for feedback
V0.3	19/4/23	Deloitte amendments
V0.4	10/5/23	Cabrini IT amendments
V0.5	7/7/23	Business SME amendments
V0.6	24/7/23	Senior Management amendments
V0.7	27/7/23	Version for Legal review
V0.8	9/11/23	Legal review
V0.9	14/12/23	Final version
V1.0	17/01/24	Final version loaded onto Prompt
V1.1	15/05/24	Fixed typos and references to previous classification levels. Amended email requirement for encryption of data in transit. Removed unnecessary definition for “confidential”.

Created by	Noel Currie	Security Program – Program Manager
	Ben Walker	Deloitte
	Islam, Tausif	Deloitte
Reviewed by	Derek Price	CIO
	Peter Matthews	Security Manager
	Chris Seymour	Director of Technology - Portfolio management
	Libby Hadjiloukas	Applications Manager
	Lee Mariu	Infrastructure Manager
	Ben Galloway	Operations Manager
	Peter O'Callaghan	Enterprise Risk Management consultant
	Liz Mines	Privacy Officer
	David Rankin	Director Clinical Governance & Informatics
	Cathy Ryan	Group Director, Health Funds and Patient Services
	Tim Staker	Chief of Cabrini Technology
	Paul Vine	General Counsel and Company Secretary
	Executive	Cabrini Executive

Executive Sponsor	**Derek Price**	
Content Approved By:	Derek Price, Updated version	**Date: 11/12/23** **Date: 16/05/24**
Authorised to Publish By:	Derek Price	**Date:** 15/1/24 **Date: 16/05/24**

Appendix A

See below for a guide on how Cabrini staff can ascertain what classification they should be applying to data types.



Appendix B

Information Asset Register

The Information Asset Register is used to estimate and record Criticality and Sensitivity levels of Information Technology assets.

Instructions

The information asset register has been adapted from a VPDSS IAR template and takes an application-centric view of digital information assets. All applications or types of systems that transmit or store digital information are to be added to this register as "assets". These applications may store or process many individual data records and are viewed collectively as "information assets".

1. Complete the basic asset information (green columns).
2. Estimate the business criticality of the asset. Using the business criticality table below as a guide, select the most appropriate criticality rating from the drop-down box (blue column).
3. Consider the nature of the asset and determine the most sensitive information type it stores or processes. Select the most appropriate choice from the drop-down box (first purple column). If there is more than one type that is relevant, select the one that is likely to result in a higher impact if the data was exposed in a breach. Note that because this relates to data sensitivity, the most important consideration is confidentiality rather than integrity or availability.
4. Consider the nature of the asset and the most sensitive type of data that it stores or processes and select the appropriate numerical impact values for a confidentiality breach of that data. Select values for financial, personal, and reputational impact respectively (remaining purple columns). Use the Business Impact table below as a guide. This table has been adapted from our enterprise risk management framework.
5. After selecting all the impact ratings, the maximum value will be calculated as the overall breach impact score, and the associated sensitivity rating will be displayed next to it (black columns). This sensitivity rating should be applied to all systems that are associated with the asset, and to the relevant data stored, processed, or exported from those assets unless redacted, de-identified, anonymized or obfuscated to lower that sensitivity rating.

Column	Notes
Asset name / description	Self explanatory. A brief name and description of the asset.
Asset creation date	Add the implementation date for new assets, otherwise "Existing".
Asset purpose / comments	Briefly state the purpose of the asset and note any important considerations.
Asset storage location	A drop down list of data storage locations to select from. This should be the primary location where the asset stores it's data.
Business owner	The business owner of the asset
Technical / operations owner	The technical or operational owner of the asset.
Business criticality	A measure of the degree to which the organisation depends on the asset.
Most sensitive information type	A drop down list containing options for the most sensitive type of data stored or processed by the asset.
Operational impact if breached	A drop down list of numerical impact ratings associated with operational impact
Financial impact if breached	A drop down list of numerical impact ratings associated with financial impact
Personal impact if breached	A drop down list of numerical impact ratings associated with personal impact
Reputational impact if breached	A drop down list of numerical impact ratings associated with reputational impact
Calculated asset breach impact score	Overall calculated breach impact score for the asset.
Calculated sensitivity rating	Overall calculated sensitivity rating for the asset.

Business Criticality	
Bronze	The service, application or infrastructure is used by small numbers of external customers or stakeholders, but the access is infrequent, and loss of the service would not have a significant impact. There are not likely to be significant impacts associated with the loss or unavailability of data associated with this service, i.e: Non-Production servers. Bronze is the default level if no other level is assigned.
Silver	Disruption of service impacts a significant number of users and impairs the business operation, but the business can still deliver its services to customers with minimal interruption. Eg: MS Teams
Gold	Disruption of service has an immediate and significant impact to critical business functions and delivery of services to customers. Business operations can continue in a restricted fashion, although long-term productivity might be adversely affected, and some service delivery to customers may be interrupted. Eg: Workday, Chris21
Platinum	Disruption of service has an immediate and severe impact to critical business functions and delivery of services to customers is severely disrupted or totally stopped. Disruption of the service is unsustainable for the business because core business operations are severely disrupted or totally stopped, and critical data is at risk of loss or corruption. Eg: PAS application / PAS Production servers

Business Impact	
Negligable - 0	**Operational:** Minimal if any operational impact. **Financial:** Negligible or no financial loss. **Personal:** No injuries. **Reputational:** Unfounded, vexatious complaints that can be dealt with routinely.
Minor - 1	**Operational:** Noticeable but limited operational impact. **Financial:** 1% of monthly revenue. **Personal:** Localised first aid required, resulting in no disability. **Reputational:** Complaints requiring written response
Moderate - 2	**Operational:** Substantial operational impact. **Financial:** 5% of monthly revenue. **Personal:** Unexpected/unplanned health impairment or physical injury. **Reputational:** Consumer complaint of any category.
Major - 3	**Operational:** Major loss of operational capability. **Financial:** 5-10% monthly revenue. **Personal:** Serious injury requiring significant medical intervention. **Reputational:** Some media attention and reputational damage.
Severe - 4	**Operational:** Complete operational failure **Financial:** > 10% monthly revenue **Personal:** Death or permanent disability. **Reputational:** Significant media attention and lasting reputational damage.

Sample of the Information Asset Register:

Asset name/description	Asset creation date (M/Y	Asset purpose / comments	Asset Storage Location	Business owner	Technical / Operations owner	Business criticality	Most sensitive information ty	Operational impact if breached	Financial impact if breached	Personal impact if breached	Reputational impact if	Calculated asset breach impact sc	Calculated sensitivity rati
3M Code finder	Existing			Health Information Services Manager (Liz Mines)	Applications Manager (Libby Hadjiloukas)	Bronze		1	1	1	1	1	Internal
3M Web Codefinder	Existing			Health Information Services Manager (Liz Mines)	Applications Manager (Libby Hadjiloukas)	Bronze		1	1	1	1	1	Internal
Access Database	Existing			Various	Database Administrator (Celia Liang)	Bronze		1	1	1	1	1	Internal