COLLEGE OF PHYSICIANS AND SURGEONS OF BRITISH COLUMBIA

Diagnostic Accreditation Program

ACCREDITATION STANDARDS

Personal Health Information/Data – Security, Management, Confidentiality and Retention

Diagnostic Accreditation Program
College of Physicians and Surgeons of British Columbia
300–669 Howe Street
Vancouver BC V6C 0B4

Introduction

Personal health information/data refers to all recorded information about an identifiable individual that is related to the individual's health or the provision of health services to the individual.

In medical imaging, the primary source of personal health information data is medical images and imaging reports; these are medical records.

Data security refers to the process of protecting personal health information/data from unauthorized access, corruption or theft.

Data management refers to the process of collecting, processing, storing and using personal health information/data.

Data residency refers to the physical location of personal health information/data. Data residency must comply with applicable provincial and federal legislation.

Personal health information/data must be kept confidential.

Personal health information/data security

No.		Description	Risk	Reference	Change
					New
DATA1.0		**PERSONAL HEALTH INFORMATION/DATA SECURITY**			
DATA1.1		**There are policies and procedures to support personal health information/data security.**			New
DATA1.1.1	**M**	There are policies and procedures for personal health information/data security. *Guidance: It is recommended that facilities refer to the ACR–AAPM–SIIM Practice Parameter for Electronic Medical Information Privacy and Security for recommendations.*	M	II-DISP-AC-24	New
DATA1.1.2	**M**	There are policies and procedures for network security. *Guidance: Network security includes, but is not limited to, firewall management, intrusion detection, bandwidth allocation and monitoring.*	M	II-DISP-AC-24	New
DATA1.1.3	**M**	There are policies and procedures for user access to systems which have personal health information/data (i.e. PACS, RIS, medical imaging systems, servers, etc.).	M	II-DISP-AC-24	New
DATA1.1.4	**M**	There are policies and procedures for the level of access of personal health information/data permitted for each category of staff. *Guidance: User access aligns with the staff's role or function.*	M	II-DISP-AC-24	New
DATA1.1.5	**M**	There are policies and procedures for password creation and protection, which includes syntax, expiration cycle and reuse specifications.	M	II-DISP-AC-24	New
DATA1.1.6	**M**	There are policies and procedures for disaster recovery/emergency operations.	M	II-DISP-AC-24	New
DATA1.1.7	**M**	There are policies and procedures for the management of security incidents and vulnerabilities.	M	II-DISP-AC-24	New
DATA1.2		**There are support resources for personal health information/data security.**			New
DATA1.2.1	**M**	There is a designated individual, or team, responsible for regularly monitoring and evaluating the effective management of the personal health information/data security.	M	II-DISP-AC-24	New
DATA1.3		**Networks are secure.**			New
DATA1.3.1	**M**	There are secure external firewalls for any network with a connection to the internet or external network.	M	II-DISP-AC-24	New

No.		Description	Risk	Reference	Change
DATA1.3.2	**B**	Networks are monitored.		II-DISP-AC-24	New
DATA1.4		**User access is restricted and monitored.**			New
DATA1.4.1	**M**	Authorized staff maintain user access and restriction controls.	M	II-DISP-AC-24	New
DATA1.4.2	**M**	User access is logged.	M	II-DISP-AC-24	New
DATA1.5		**Passwords are secure.**			New
DATA1.5.1	**M**	Generic logins are not used to access PACS/MIMPS and RIS/HIS.	M	II-DISP-AC-24	New
DATA1.6		**Data can be recovered in the event of a disaster/emergency.**			New
DATA1.6.1	**B**	The disaster recovery procedure has been trialed.		II-DISP-AC-24	New
DATA1.7		**Security incidents and vulnerabilities are resolved.**			New
DATA1.7.1	**M**	Security incidents and vulnerabilities are documented, investigated and resolved.	M	II-DISP-AC-24	New

Personal health information/data management

No.		Description	Risk	Reference	Change
					New
DATA2.0		**PERSONAL HEALTH INFORMATION/DATA MANAGEMENT**			
DATA2.1		**Data integrity is monitored and maintained.**			New
DATA2.1.1	**M**	There are policies and procedures for the management of data errors, data deletion and patient identification errors (i.e. patient/examination mismatch).	M	II-DISP-AC-24	New
DATA2.1.2	**M**	Corrections/reconciliation is performed by authorized individuals.	M	II-DISP-AC-24	New
DATA2.1.3	**M**	Health-care providers who have viewed incorrect personal health information/data are notified.	M	II-DISP-AC-24	New
DATA2.1.4	**M**	Personal health information/data that is entered manually is verified for accuracy.	M	II-DISP-AC-24	New
DATA2.1.5	**M**	Personal health information/data records which are digitally transmitted from external organizations are validated.	M	II-DISP-AC-24	New
DATA2.1.6	**M**	Personal health information/data records (digital and hard copy) include patient identification (i.e. name, unique identifier, personal health number).	M	II-DISP-AC-24	New
DATA2.1.7	**M**	Personal health information/data records (digital and hard copy) include examination identification (i.e. examination type, date, accession number, facility).	M	II-DISP-AC-24	New
DATA2.2		**Data is recoverable.**			New
DATA2.2.1	**M**	Medical imaging database backups are performed daily.	M	II-DISP-AC-24	New
DATA2.2.2	**M**	Medical imaging database backups are located in a separate physical location.	M	II-DISP-AC-24	New
DATA2.3		**Network and servers support data availability.**			New
DATA2.3.1	**M**	There are high availability servers.	M	II-DISP-AC-24	New
DATA2.3.2	**M**	Servers are maintained in accordance with the manufacturer's recommendations.	M	II-DISP-AC-24	New
DATA2.3.3	**B**	Network architecture and server capacity ensure prompt data availability. *Guidance: The timeliness of data availability must meet the requirements of the user, as achievable.*		II-DISP-AC-24	New
DATA2.4		**Data is stored.**			New
DATA2.4.1	**M**	Data storage capacity planning is periodically performed to ensure the storage needs of the facility are maintained.	M	II-DISP-AC-24	New

No.		Description	Risk	Reference	Change
DATA2.4.2	**M**	Data is stored and in an environment that is secure from unauthorized access and safeguarded from physical damage (e.g. water, fire).	M	II-DISP-AC-24	New
DATA2.4.3	**M**	Data residency complies with applicable provincial and federal legislation. Data residency refers to the geographical location of personal health information/data. *Guidance: The BC Freedom of Information and Protection of Privacy Act was amended in 2021 to allow public bodies (ministry and non-ministry) to store sensitive personal information outside of Canada following a privacy impact assessment. Refer to the Ministry's Guidance on Disclosures Outside of Canada (https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/privacy/privacy-impact-assessments/guidance-on-disclosures-outside-of-canada). Private sector health services must ensure compliance with the Personal Information Protection Act and it is recommended that privacy impact assessments are conducted when data residency is outside of Canada. Private sector health services may wish to refer to https://www.oipc.bc.ca/documents/guidance-documents/2246. Data residency and privacy legislation is under review provincially and federally, and new legislation may supersede any statement in this guidance upon issue. It is recommended that medicolegal guidance is obtained if personal health information/data is stored outside of Canada.*	M	II-DISP-AC-24	New
DATA2.5		**Data is managed during system downtimes.** *Guidance: Systems includes all systems which have patient health information/data (i.e. PACS/MIMPS, RIS, HIS, EMR, imaging systems, computers, etc.).*			New
DATA2.5.1	**M**	There are policies and procedures for the management and recovery of data during scheduled and unscheduled system downtimes.	M	II-DISP-AC-24	New
DATA2.5.2	**M**	Downtime policy and procedures are readily accessible.	M	II-DISP-AC-24	New
DATA2.5.3	**M**	Unscheduled system downtimes are documented.	M	II-DISP-AC-24	New
DATA2.6		**Image data compression is appropriate for the clinical task.**			New
DATA2.6.1	**M**	If irreversible (lossy) compression is applied there is a process to validate that the image quality is sufficient to reliably perform the clinical task. *Guidance: The type of body part, the modality, and the objective of the study will determine the amount of compression that can be tolerated.*	M	ACR-AAPM-SIIM-TS.Electronic.MI	New

No.		Description	Risk	Reference	Change
DATA2.6.2	**M**	If irreversible (lossy) compression is applied, the image displays that irreversible compression has been applied, the approximate compression ratio and the type of standard compression scheme (i.e. JPEG).	M	ACR-AAPM-SIIM-TS.Electronic.MI	New
DATA2.6.3	**M**	Irreversible (lossy) compression is not applied to mammography imaging.	M	ACR-AAPM-SIIM-TS.Electronic.MI	New
DATA2.7		**The use of portable media devices (CDs/DVDs and USBs) is restricted and controlled.**			New
DATA2.7.1	**M**	Portable media devices include user viewing instructions.	M	II-DISP-AC-24	New
DATA2.7.2	**M**	Portable media devices are labelled with a patient identifier, a confidential medical records statement and instructions for unintended recipients.	M	II-DISP-AC-24	New
DATA2.7.3	**M**	Portable media devices are not used for data archive purposes.	M	II-DISP-AC-24	New
DATA2.7.4	**M**	Portable media devices used as temporary data backups are encrypted and password protected. *Guidance: In rare circumstances, the imaging service may not have immediate access to a secured database server (through a PACS system). If image data is temporarily stored to portable media (USB media, DVD, CD), the facility has implemented strict measures to maintain the security of the data.*	M	II-DISP-AC-24	New
DATA2.7.5	**M**	Portable media devices conform to the Integrating the Healthcare Enterprise (IHE) Portable Data for Imaging (PDI) integration profile.	M	II-DISP-AC-24	New
DATA2.8		**Data sharing is secure and integrated with external organizations.**			New
DATA2.8.1	**B**	Images and reports are securely shared with external organizations digitally, when processes for the digital communication of data with external organizations are available and secure (i.e. pushing to the grid). *Guidance: The sharing of images and reports as portable media is discouraged when processes for the digital communication of data with external organizations are available and secure. If portable media is used see DATA2.7 for requirements.*		II-DISP-AC-24	New
DATA2.9		**Data is destroyed.**			New
DATA2.9.1	**M**	There is a policy and procedure for the destruction of data, in alignment with the organization's retention policy and applicable law.	M	II-DISP-AC-24	New

Personal health information/data confidentiality

No.		Description	Risk	Reference	Change
					New
DATA3.0		**PERSONAL HEALTH INFORMATION/DATA CONFIDENTIALITY**			
DATA3.1		**Patient information is confidential.**			New
DATA3.1.1	**M**	There are policies and procedures for the use, release and disclosure of patient information. *Intent: The policy must include the release of information to patients, family, other service areas, other organizations, for research or education purposes or legal reasons.*	M	II-DISP-AC-24	New
DATA3.1.2	**M**	Applicable patient identifiers are removed from images and reports, when released for research, educational and or marketing purposes.	M	II-DISP-AC-24	New
DATA3.1.3	**M**	Release of patient information complies with applicable provincial and federal legislation.	M	II-DISP-AC-24	New
DATA3.1.4	**M**	There are policies and procedures for the management of unauthorized access to patient information. *Guidance: An example of unauthorized access to patient information includes when a health-care provider views patient information not related to their care (i.e. family members).*	M	II-DISP-AC-24	New

Personal health information/data retention

No.		Description	Risk	Reference	Change
DATA4.0		**THE DIAGNOSTIC SERVICE RETAINS DOCUMENTS AND RECORDS.**			New
DATA4.1		**Retention of personal health information/data complies with policy and applicable law.**			New
DATA4.1.1	**M**	Medical records are retained according to British Columbia's revised *Limitation Act* (2013). *Guidance: The medical record comprises all the clinical data and information related to the patient's diagnostic procedure. The medical record contains all relevant documents for testing including, but not limited to the request, hard copy or electronic worksheets, reports and images. Facilities and medical leaders establishing retention times outside of the requirements of the Limitation Act should seek and act according to expert legal advice on this matter.*	M	II-DISP-AC-24	New

References

Abbreviation	Citation
ACR-AAPM-SIIM-TS.Electronic.MI	American College of Radiology (ACR), the American Association of Physicists in Medicine (AAPM), and the Society for Imaging Informatics in Medicine (SIIM). ACR–AAPM–SIIM Technical Standard For Electronic Practice Of Medical Imaging [Internet]. [Virginia]: American College of Radiology; 2007 [rev 2022, amend 2023]. Available from: https://www.acr.org/-/media/ACR/Files/Practice-Parameters/Elec-Practice-MedImag.pdf
II-DISP-AC-24	2024 DAP Imaging Informatics, Displays, PACS Advisory Committee Recommendation

Bibliography

American Association of Physicists in Medicine. AAPM Report No. 270 Display Quality Assurance [Internet]. [Virginia]: American Association of Physicists in Medicine; 2019. Available from: https://www.aapm.org/pubs/reports/RPT_270.pdf

American College of Radiology (ACR), the American Association of Physicists in Medicine (AAPM), and the Society for Imaging Informatics in Medicine (SIIM). ACR–AAPM–SIIM Practice Parameter for Electronic Medical Information Privacy And Security [Internet]. [Virginia]: American College of Radiology; 2004 [rev 2019, amend 2023]. Available from: https://www.acr.org/-/media/ACR/Files/Practice-Parameters/Elec-Info-Privacy.pdf

American College of Radiology (ACR), the American Association of Physicists in Medicine (AAPM), and the Society for Imaging Informatics in Medicine (SIIM). ACR–AAPM–SIIM Technical Standard For Electronic Practice Of Medical Imaging [Internet]. [Virginia]: American College of Radiology; 2007 [rev 2022, amend 2023]. Available from: https://www.acr.org/-/media/ACR/Files/Practice-Parameters/Elec-Practice-MedImag.pdf

American College of Radiology (ACR), the American Association of Physicists in Medicine (AAPM), the Society for Imaging Informatics in Medicine (SIIM) and the Society for Pediatric Radiology (SPR). ACR–AAPM–SIIM-SPR Practice Parameter for Digital Radiography [Internet]. [Virginia]: American College of Radiology; 2007 [rev 2022, amend 2023]. Available from: https://www.acr.org/-/media/ACR/Files/Practice-Parameters/rad-digital.pdf

American College of Radiology (ACR), the American Association of Physicists in Medicine (AAPM), and the Society for Imaging Informatics in Medicine (SIIM). ACR–AAPM–SIIM Practice Parameter for Determinants of Image Quality In Mammography [Internet]. [Virginia]: American College of Radiology; 2007 [rev 2022, amend 2023]. Available from: https://www.acr.org/-/media/ACR/Files/Practice-Parameters/Dig-Mamo.pdf

Canadian Standards Association. CSA Z8000:23 Canadian health care facilities. Ontario: CSA Group; 2023.