

**Division: D- PRIVACY AND SECURITY****POLICY: INFORMATION HANDLING, SECURITY AND DISPOSAL****Original Date:** January 17, 2007**Revision Date:**

Reviewed Date: October 22, 2020

**Signatures:** *Wendy Martin - Gutjahr, CEO*POLICY  
D – 40 - 0**1.0 Purpose**

The information security provisions of the Health Information Act (HIA) require BGSA Radiology Inc. to protect personal health information or records in its custody or control by making reasonable security arrangements to protect against unauthorized access, collection, use, disclosure or destruction. This policy outlines administrative, technical and physical safeguards to protect confidential information.

**2.0 Scope****2.1 This policy applies to:**

- a) BGSA Radiology Inc. physicians and staff, including contractors, students, and volunteers providing services on behalf of BGSA Radiology Inc.
- b) Information or records, in whatever form or medium (paper, digital, audio-visual, graphic) created or received in the course of carrying out BGSA Radiology Inc.'s mandated functions and activities
- c) All facilities and equipment required to collect, manipulate, transport, transmit, or keep BGSA Radiology Inc. information

**3.0 Administrative Safeguards**

- 3.1 BGSA Radiology Inc. shall ensure policies and procedures, which facilitate the safeguarding of confidential information in its custody or control, are developed and maintained.
- 3.2 The need for confidentiality and security of information shall be addressed as part of the conditions of employment for BGSA Radiology Inc. staff, beginning with the recruitment stage, and included as part of job descriptions and contracts. The performance of individuals shall be monitored to reduce the risk of error, fraud, or misuse of information. All staff must be aware of, and appropriately trained with regard to, policies and procedures for safeguarding information.
- 3.3 Patients and visitors shall be accompanied by a staff member to private or semi-private Clinic areas such as examination rooms / physician offices. It is not required that a staff member waits with them in the room/ office.
- 3.4 All BGSA Radiology Inc. staff, volunteers, and contracted personnel that collect, use or disclose confidential information or records as part of the

performance of their duties for BGSA Radiology Inc. shall be required to sign a Confidentiality agreement.

- 3.5 Only the least amount of information necessary for the intended purpose should be used or disclosed, and only to staff with a need to know. If the intended purpose can be accomplished without use or disclosure of identifying information, then the information should be made anonymous.
  - 3.6 Confidential information should not be transmitted verbally if conversations can be overheard or intercepted.
  - 3.7 Before implementing proposed new administrative practices or information systems related to the collection, use and disclosure of health information or records, BGSA Radiology Inc. shall complete a privacy impact assessment (PIA) for submission to the Office of the Information and Privacy Commissioner. A PIA will describe how the new initiative will affect privacy, and what measures BGSA will put in place to mitigate risks to privacy.
  - 3.8 BGSA Radiology Inc. staff and persons acting on behalf of BGSA shall report all violations and breaches of information security as soon as possible to the Clinical Manager. This is for the purpose that corrective action can be taken to resolve the immediate problem and minimize the risk of future occurrence. The nature of the response, which may include termination, will be determined according to the level of gravity of the breach / violation.
- 4.0 Technical Safeguards
- 4.1 All BGSA Radiology Inc. information system users are assigned a unique identifier (User ID). The unique identifier restricts access to data and application systems to that information required for the administration of the their duties.
  - 4.2 BGSA Radiology Inc. staff members and affiliates shall only access and use information systems under their assigned User ID. The use of another person's assigned User ID is prohibited.
  - 4.3 Access to BGSA Radiology Inc. information systems is controlled and password protected. Passwords are to be kept confidential at all times and should not be written down, posted publicly, or shared with other staff. Passwords should be changed every 6 months.
  - 4.4 Confidential business or identifiable personal information shall not be sent via e-mail over public or external networks without the use of appropriate security measures such as encryption.
  - 4.5 To detect unauthorized access and prevent modification or misuse of user data in applications, systems shall be monitored to ensure conformity to access policies and standards. Appropriate security controls, such as audit trails, shall be designed, implemented, and reviewed every 6 months.
  - 4.6 Computer systems that hold critical or sensitive information shall be backed up on a daily basis. Backed up information is stored in a secure environment. Information that is intended for long-term storage on electronic media (e.g. tape) shall be reviewed on an annual basis to ensure

that data is retrievable, and to migrate the data to another storage medium if necessary.

## 5.0 Physical Safeguards

- 5.1 All BGSA Radiology Inc. records, both on-site and off site, shall be held and stored in an organized, safe and secure manner in accordance with information security standards. Areas where confidential patient information is stored shall be equipped with smoke detectors and fire extinguishers.
- 5.2 Appropriate measures shall be taken to control the distribution of keys, and to ensure staff returns them after their employment by the Clinic has ended.
- 5.3 Confidential information shall not be displayed in open areas; computer monitors located in public areas shall be positioned so that the general public can not view information. Privacy screens shall be used where necessary to prevent individuals from viewing confidential information unless looking directly at the screen.
- 5.4 Confidential, restricted, or sensitive information that is transmitted between BGSA Radiology Inc. affiliates, or other custodians, shall be sealed, marked as confidential, and directed to the attention of the authorized recipient. All information or records that are transmitted digitally shall be encrypted and password protected.
- 5.5 BGSA Radiology Inc. staff must verify the identity and credentials of courier services used for the transportation of personal health information.
- 5.6 Fax machines that may be used to send or receive confidential information shall be located in a secure area. Whenever possible staff should use preprogrammed numbers to send fax transmissions, and must review the numbers every 6 months to ensure they are still accurate. All fax transmissions shall be sent with a cover sheet indicating the information being sent is confidential. Reasonable steps must be made to confirm that confidential information transmitted via fax is sent to a recipient with a secure fax machine.
- 5.7 Information that is not confidential or sensitive in nature should be disposed of by placing it in recycling bins. Confidential or sensitive information shall be disposed of by shredding.
- 5.8 All information shall be wiped clean prior to disposal of electronic data storage devices (e.g. surplus computers, internal and external hard drives, diskettes, tapes, CD-ROMS etc) or the device(s) must be destroyed.
- 5.9 Patient health information, in any format (hard copy or electronic), is retained for a minimum of 10 years following the last documented contact with the patient or, in the case of a minor patient, for 2 years after the patient reaches the age of majority.