The Center for Women's Health
COASTAL IMAGING

Patient Data Privacy Policy

1. Purpose

This Patient Data Privacy Policy establishes the principles and procedures governing the collection, use, storage, and protection of patient information within The Center for Women's Health. The organization is committed to safeguarding patient privacy and ensuring compliance with all applicable laws and regulations, including HIPAA.

2. Scope

This policy applies to:

- All employees, contractors, and affiliated healthcare professionals
- All systems, applications, and devices used to access or store patient data
- All forms of patient information, including electronic, paper, and verbal communications

3. Definitions

- Protected Health Information (PHI): Any information that identifies a patient and relates to their health condition, treatment, or payment
- De-identified Data: Data stripped of identifiers such that individuals cannot be readily identified
- Minimum Necessary Standard: Access to PHI should be limited to the least amount required to perform job duties

4. Types of Data Collected

The organization may collect and process the following patient data:

- Demographic information (name, DOB, address, contact details)
- Clinical information (medical history, imaging results, radiology reports)
- Diagnostic images (mammography, ultrasound, and related imaging studies)
- Billing and insurance information
- Referring physician and care coordination data

5. Use of Patient Data

Patient data is used strictly for:

- Diagnosis and treatment
- Radiological interpretation and reporting
- Care coordination with referring providers
- Billing and payment processing
- Quality assurance and operational improvement
- Regulatory compliance and reporting

Data will not be used for unauthorized purposes, including marketing, without explicit patient consent where required.

6. Data Access and Authorization

- Access to patient data is role-based and restricted according to job function
- All workforce members must authenticate using secure credentials
- Access logs are maintained and regularly audited
- Unauthorized access or disclosure is strictly prohibited

7. Data Storage and Security

The organization implements administrative, technical, and physical safeguards, including:

- Encryption of data at rest and in transit
- Secure PACS and RIS systems
- Firewalls and intrusion detection systems
- Secure data centers and controlled physical access
- Regular system updates and vulnerability assessments

8. Data Sharing and Disclosure

Patient data may be shared only:

- With authorized healthcare providers involved in patient care
- With insurance companies for billing purposes

• As required by law (e.g., public health reporting, court orders)

• With business associates under signed agreements ensuring data protection

All disclosures must comply with applicable legal and regulatory requirements.

9. Patient Rights

Patients have the right to:

• Access and obtain copies of their records

• Request corrections to inaccurate information

• Request restrictions on certain uses or disclosures

• Receive an accounting of disclosures

• Request confidential communications

• File complaints without retaliation

Requests must be processed in accordance with regulatory timelines.

10. Data Retention and Disposal

• Patient data is retained according to federal and state retention requirements

• Secure destruction methods (e.g., shredding, digital wiping) are used when data is no longer required

11. Incident Response and Breach Notification

• Any suspected data breach must be reported immediately to the Privacy Officer

• Incidents are investigated promptly

• Affected individuals and regulatory bodies are notified as required by law

• Corrective actions are implemented to prevent recurrence

12. Workforce Training and Compliance

• All personnel must complete privacy and security training upon hire and annually thereafter

• Non-compliance may result in disciplinary action, up to and including termination

13. Third-Party Vendors (Business Associates)

• All vendors handling PHI must sign Business Associate Agreements (BAAs)

• Vendors must demonstrate adequate security controls and compliance

14. Policy Review and Updates

This policy is reviewed at least annually and updated as needed to reflect:

• Regulatory changes

• Technological advancements

• Organizational changes

15. Contact Information

Privacy Officer: Chris Cribbs

Organization: The Center for Women's Health

Phone: (912) 303-5470

Address: 105 Grand Central Blvd Suite 106, Pooler, GA 31322