DEPARTMENT: Information Protection	**POLICY DESCRIPTION:** Privacy Official
PAGE: 1 of 3	**REPLACES POLICY DATED:** 3/1/02, 4/14/03, 5/31/04, 3/1/08, 9/23/09
EFFECTIVE DATE: March 1, 2013	**REFERENCE NUMBER:** IP.PRI.002 (formerly HIM.PRI.002)
APPROVED BY: Ethics and Compliance Policy Committee	

SCOPE: All Company-affiliated facilities including, but not limited to, hospitals, ambulatory surgery centers, imaging and oncology centers, physician practices, and shared services centers.

PURPOSE: To ensure each Company-affiliated facility has a Facility Privacy Official (FPO), to meet the requirement of the HIPAA Privacy Standard (§164.530) and to ensure each Company-affiliated hospital and shared services center (SSC) establishes or identifies an existing committee to be designated with the facility's Privacy Program oversight.

To establish the requirements for each Company-affiliated facility to protect patients' privacy rights and their individually identifiable health information as required by the Health Insurance Portability and Accountability Act (HIPAA), Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164 and all Federal regulations and interpretive guidelines promulgated thereunder.

POLICY: Each Company-affiliated facility must have an FPO to oversee and implement the Privacy Program and work to ensure the facility's compliance with the requirements of the HIPAA Standards for Privacy of Individually Identifiable Health Information. The FPO must be informed of all complaints about matters of Patient Privacy that are received by the facility.

- Multiple facilities may choose to appoint one FPO to cover each of their Privacy Programs (*e.g.*, Area Practice Mangers, hospital markets); however, each facility must have its own distinct Privacy Program.

The FPO must be informed of all privacy complaints and all Office of Civil Rights privacy investigations.

Each FPO at a Company-affiliated hospital and service center must:

- Establish or identify an existing committee to be designated with Privacy Program oversight and responsibility, and
- Be a member of the Facility Ethics and Compliance Committee and/or the Facility Security Committee for reporting and accountability purposes.

PROCEDURE:

1. Each Chief Executive Officer (CEO), Administrator or Area Practice Manager of a Company-affiliated facility shall designate an appropriate individual to serve as the FPO. Notice of who will serve as FPO must be provided to the Company Privacy Officer by e-mailing the Privacy Official Add/Change Form to the HIPAA Communication mailbox anytime there is a change in such position.

2. Each FPO must oversee and implement the Company's and facility's Privacy Program and work to ensure compliance with the requirements of the HIPAA Privacy Standards.

DEPARTMENT: Information Protection	**POLICY DESCRIPTION:** Privacy Official
PAGE: 2 of 3	**REPLACES POLICY DATED:** 3/1/02, 4/14/03, 5/31/04, 3/1/08, 9/23/09
EFFECTIVE DATE: March 1, 2013	**REFERENCE NUMBER:** IP.PRI.002 (formerly HIM.PRI.002)
APPROVED BY: Ethics and Compliance Policy Committee	

3. The FPO responsibilities for implementation and oversight of the Privacy Program include but are not limited to:

   a. Privacy Policies and Standards
      i. Assisting with communication and implementation of the Privacy Program to the facility's workforce.
      ii. Assisting with facility-wide deployment, implementation and compliance with the Company-wide policies and procedures (IP.PRI.001-IP.PRI.013) related to privacy.
      iii. Developing, revising, communicating, implementing, and complying with facility-specific policies and procedures related to patient privacy.

   b. Training
      i. Overseeing initial and ongoing training for all facility workforce members on the policies and procedures related to protected health information as necessary and appropriate to carry out their job-related duties, and that training is promptly provided if there are any changes to the policies or procedures.
      ii. Ensuring all new members of the workforce are trained within a reasonable period of time, preferably during initial orientation training.
      iii. Ensuring documentation that initial and ongoing training has been provided to each workforce member is retained.

   c. Advising members of the workforce on privacy matters as appropriate.

   d. Complaints
      i. Serving as the individual to receive complaints concerning privacy rights.
      ii. In conjunction with other appropriate parties (*e.g.*, Human Resources, ECO, department heads) investigating the complaint.
      iii. Documenting complaints received and their disposition.
      iv. Maintaining a log of privacy complaints.
      v. Incorporating the complaint process into the facility grievance process as required by the Centers for Medicare and Medicaid Service's (CMS) Conditions of Participation.

   e. Protected Health Information Breach Notification Requirements
      In the event a disclosure is discovered and the breach meets the definition as outlined in the Protected Health Information Breach Notification Policy, IP.PRI.011, and the American Recovery and Reinvestment Act of 2009, executing the requirements as outlined in IP.PRI.011.

DEPARTMENT: Information Protection	**POLICY DESCRIPTION:** Privacy Official
PAGE: 3 of 3	**REPLACES POLICY DATED:** 3/1/02, 4/14/03, 5/31/04, 3/1/08, 9/23/09
EFFECTIVE DATE: March 1, 2013	**REFERENCE NUMBER:** IP.PRI.002 (formerly HIM.PRI.002)
APPROVED BY: Ethics and Compliance Policy Committee	

f. Sanctions
   i. In conjunction with the appropriate manager, ensuring violations of privacy policies and procedures are addressed as appropriate pursuant to the Company's Code of Conduct, facility HR policies and procedures and the facility's privacy and security sanctions policy.
   ii. Documenting sanctions that are applied.

g. Mitigating, to the extent practicable, any harmful effect that is known to the Company or facility from the use or disclosure of protected health information in violation of policies and procedures.

h. Ensuring any documentation required by the privacy policies and program is kept for a minimum of six (6) years from the effective or change date pursuant to the Records Management Policy, EC.014.

REFERENCES:

1. Health Insurance Portability and Accountability Act (HIPAA), Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164
2. American Recovery and Reinvestment Act of 2009, Title XIII, Subtitle D
3. Patient Privacy Program Requirements Policy, IP.PRI.001
4. Protected Health Information Breach Notification Policy, IP.PRI.011
5. Records Management Policy, EC.014
6. FPO Checklist
7. Privacy Official Add/Change Form