OUR MISSION

To ensure institutional compliance with federal and state privacy regulations, as well as industry standards, for restricted information. To provide centralized resources, oversight and enforcement recommendations for privacy-related activities.

OUR CORE RESPONSIBILITIES

1. To develop, implement, and maintain University privacy-focused policies, procedures and guidelines that comply with statutory mandates and industry regulations.

2. To deliver privacy-related training and to oversee privacy program monitoring and enforcement as required by privacy statutes and standards.

3. To serve as the central contact and investigation authority for privacy complaints, incidents, and breaches. To coordinate the privacy notifications when required.

4. To evaluate opportunities to reduce privacy risks and to execute program modifications that advance overall privacy compliance.

5. To coordinate University medical records management and to provide consultation as University clinics transition to electronic medical record systems.

I. Direct, Manage, and Monitor UF Privacy Office “operations.”

- Act to ensure University-related privacy issues receive immediate expert attention.
  - Participate in campus-wide initiatives where “privacy” becomes key concern.
  - Establish campus-representative Privacy Advisory Council.
  - Create “privacy statement” policy criteria and monitor compliance cross-campus.

- Supervise Privacy Offices at existing University campus locations.

- Establish “Excellence” program for Office staff and institute succession plan.
  - Support participation in professional organizations by paying dues, subscriptions, or conference attendance.
  - Offer career development with cost-sharing options for classes, seminars, workshops, or other educational programs.
  - Provide funding for approved privacy-related certifications.

- Mitigate privacy compliance risks through training and policy revision.

- Conduct investigations of all reported privacy breaches, including but not limited to HIPAA incidents-complaints-violations, and resolve privacy-related violations through sanctions-disciplinary measures-corrective actions.

- Continue ‘Monitoring and Auditing Plan’ implementation for regulatory compliance; implement audits that are staged by risk priority and trigger events.

- Monitor the HIPAA research protocol or waiver reviews conducted by IRB administrative analysts. Enforce HIPAA sanctions for research compliance by partnering with IRBs-Privacy Boards.
- Provide regular status reporting to Vice President of Human Resources and as needed to University executive leadership.

II. **Improve Privacy Management efficacy by automation or collaboration with other University agents, key stakeholders and partners.**

- Complete the reconstruction of the University privacy website to include privacy information by stakeholder or data group.
- Explore collaborative opportunities with University Security Administration, similar to governance of Business Associate Agreements for Privacy and Security.
- Continue to trim privacy-related operating expenses by redesign of work processes.

III. **Manage individual notification for University organizations when a personal data breach occurs.**

- Create, maintain, and communicate policy and procedures for breach notification processes.
- Track the notification efforts by organization and report notification activities to University administration.
- Act as coordinator or liaison when external agencies require privacy breach information.

IV. **Act as Health Science Center Medical Records Coordinator to preserve the confidentiality and integrity of UF clinic medical records.**

- Write and implement medical records policy as required. Coordinate medical records practices with healthcare system partners.
Coordinate developing medical records disaster recovery plans for faculty practice groups.

Provide consultation and evaluation assistance to Faculty Practice groups and other organizations as electronic medical record systems are constructed.

PRIVACY CHALLENGES

The year forward brings new opportunities to build on what we have accomplished and address the next phase of Privacy initiatives. Among the privacy issues that will continue to present change and challenge are:

- International Privacy Regulations
- Big Data Initiatives
- Research “HIPAA” Compliance
- Privacy and Social Media Exposures
- Interstate Telemedicine Activities

PRIVACY OFFICE TEAM

- Susan Blair, MSJ, MBA, CIPP, CCEP, CIA: Chief Privacy Officer, University of Florida all campus and extension sites
- Cheryl Webber, MS, RHIA: Privacy Manager, Jacksonville.*
- Mary Anne Norris, MIB, CIA: Privacy Auditor.
- Caroel DeBose, MBA: The NPI Project Coordinator/Privacy Analyst.
- Kameelah Spence, MS: Privacy Analyst.*

* New Hire April 7, 2014.