The Office of the National Coordinator for Health Information Technology

First Annual Summary of Privacy and Security Tiger Team Activities

July 1, 2010 through September 30, 2013

Office of the Chief Privacy Officer

The Office of the National Coordinator for Health Information Technology

Privacy and Security Tiger Team

- The Privacy and Security Tiger Team is a workgroup of the Health Information Technology Policy Committee (HITPC), a federal advisory committee. The Tiger Team is charged with making short-term and long-term recommendations to the HITPC on privacy and security policies and practices that will help build public trust in health IT and electronic health information exchange (HIE). Approved recommendations are sent to the Office of the National Coordinator for Health Information Technology (ONC) for possible action.
  - View additional information about the HITPC: http://www.healthit.gov/policy-researchers-implementers/health-it-policy-committee

- The Tiger Team was formed in 2010 to enable quick progress in advising ONC on critical privacy and security issues facing the nation as it moves toward the adoption of electronic health records (EHR) and HIE.
  - View additional information about the Tiger Team: http://www.healthit.gov/policy-researchers-implementers/federal-advisory-committees-facas/privacy-security-tiger-team

Tiger Team Members

As of September 30, 2013

- Deven McGraw, Chair, Center for Democracy & Technology
- Paul Egerman, Co-Chair
- Dixie Baker, Martin, Blanck, and Associates
- Judy Faulkner, Epic
- Leslie Francis, University of Utah College of Law
- Gayle Harrell, Consumer Representative/Florida
- John Houston, University of Pittsburgh Medical Center
- David McCallie, Cerner Corporation
- Wes Rishel, Gartner
- Micky Tripathi, Massachusetts eHealth Collaborative
- Kitt Winter, Social Security Administration
- David Holtzman, OCR, Ex-Officio

Former Tiger Team Members

- Christine Bechtel, National Partnership for Women & Families
- Rachel Block, NYS Department of Health
- Dan Callahan, Social Security Administration
- Neil Calman, Institute for Family Health
- Carol Diamond, Markle Foundation
- David Lansky, Pacific Business Group on Health
- Alice Leiter, National Partnership for Women & Families
- Latanya Sweeney, Carnegie Mellon University
- Adam Greene, OCR, Ex-Officio
- Verne Rinker, OCR, Ex-Officio

Foundation for Tiger Team Recommendations*

The Tiger Team's recommendations are based on **Fair Information Practice Principles**

Simple ways to get
Individual Access
to one's health information

ability to make a
Correction
to one's health information

Individual Choice
about how health information is used

Openness and Transparency
about policies, procedures, and technologies
that affect patients and their health information

health information is subject to
Collection, Use and Disclosure Limitations

Safeguards
to ensure confidentiality
and control access

Data Quality and Integrity
of health information

Accountability
for adherence to these principles

*The Tiger Team used the formulation of the Fair Information Practice Principles (FIPPs) endorsed by the HIT Policy Committee and adopted by ONC in the *Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information.*
http://www.healthit.gov/sites/default/files/nationwide-ps-framework-5.pdf

Core Guiding Values

- The relationship between the patient and his or her health care provider is the foundation for trust in health information exchange, particularly with respect to protecting the confidentially of personal health information.

- As key agents of trust for patients, providers are responsible for maintaining the privacy and security of their patients' records.

- We must consider patient needs and expectations. Patients should not be surprised about or harmed by collections, uses, or disclosures of their information.

- Ultimately, to be successful in the use of health information exchange to improve health and health care, we need to earn the trust of both consumers and physicians.

Major Public Hearings

- Accounting of Disclosures (September 30, 2013)*
- Non-Targeted Queries (June 24, 2013)
- Trusted Identity of Patients in Cyberspace** (November 29, 2012)
- Trusted Identity of Physicians In Cyberspace** (July 11, 2012)
- Patient Matching (December 9, 2010)
- Consumer Choice Technology (June 20, 2010)

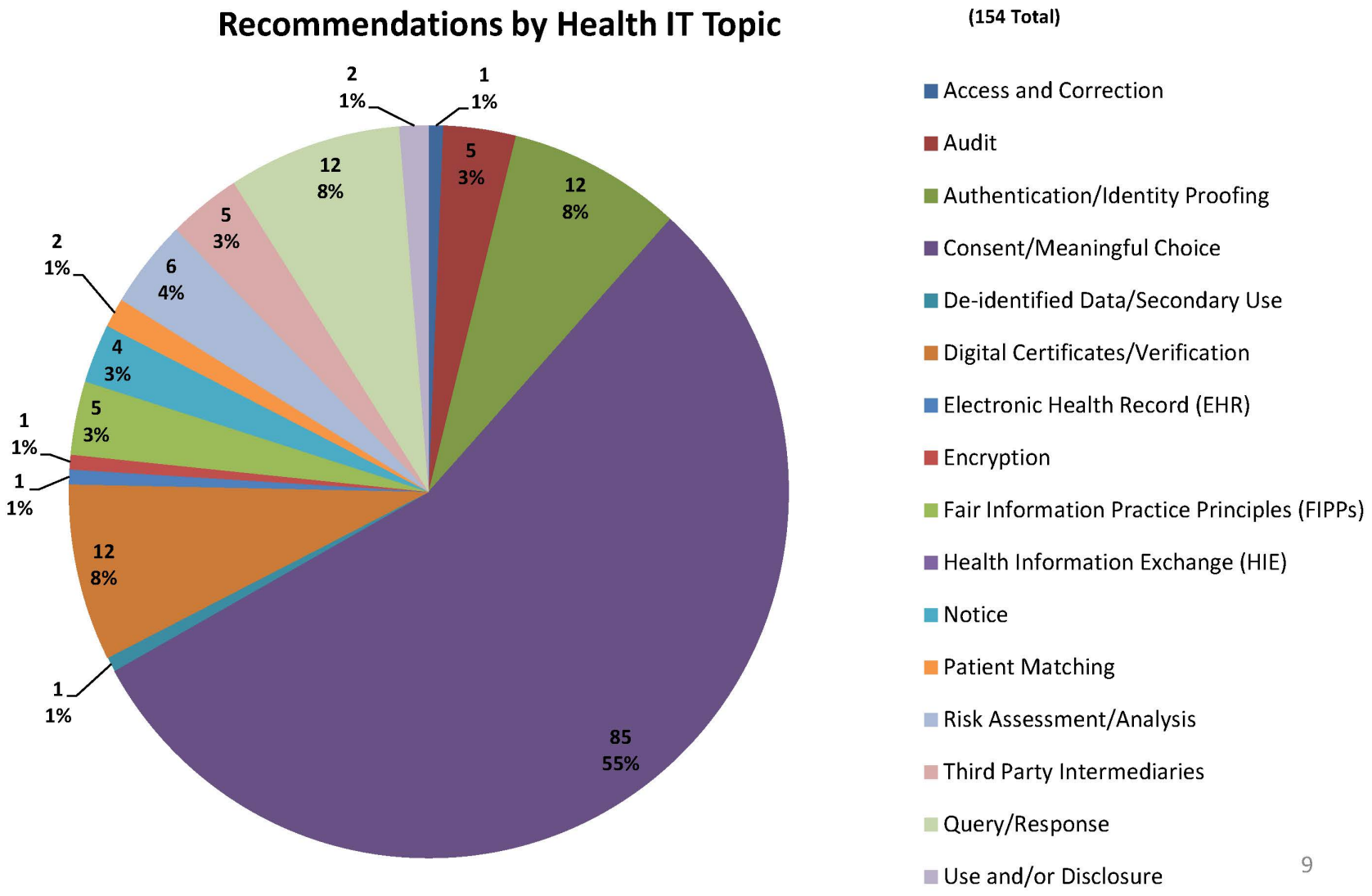
*Coordinated with National Committee on Vital and Health Statistics (NCVHS) and the HITSC Privacy and Security Workgroup
**Joint hearing with HITSC Privacy and Security Workgroup

160 Total Tiger Team Recommendations

- 154 recommendations were approved by the HITPC and transmitted to ONC

- 6 recommendations were withdrawn by the Tiger Team as no longer relevant due to ONC actions already taken

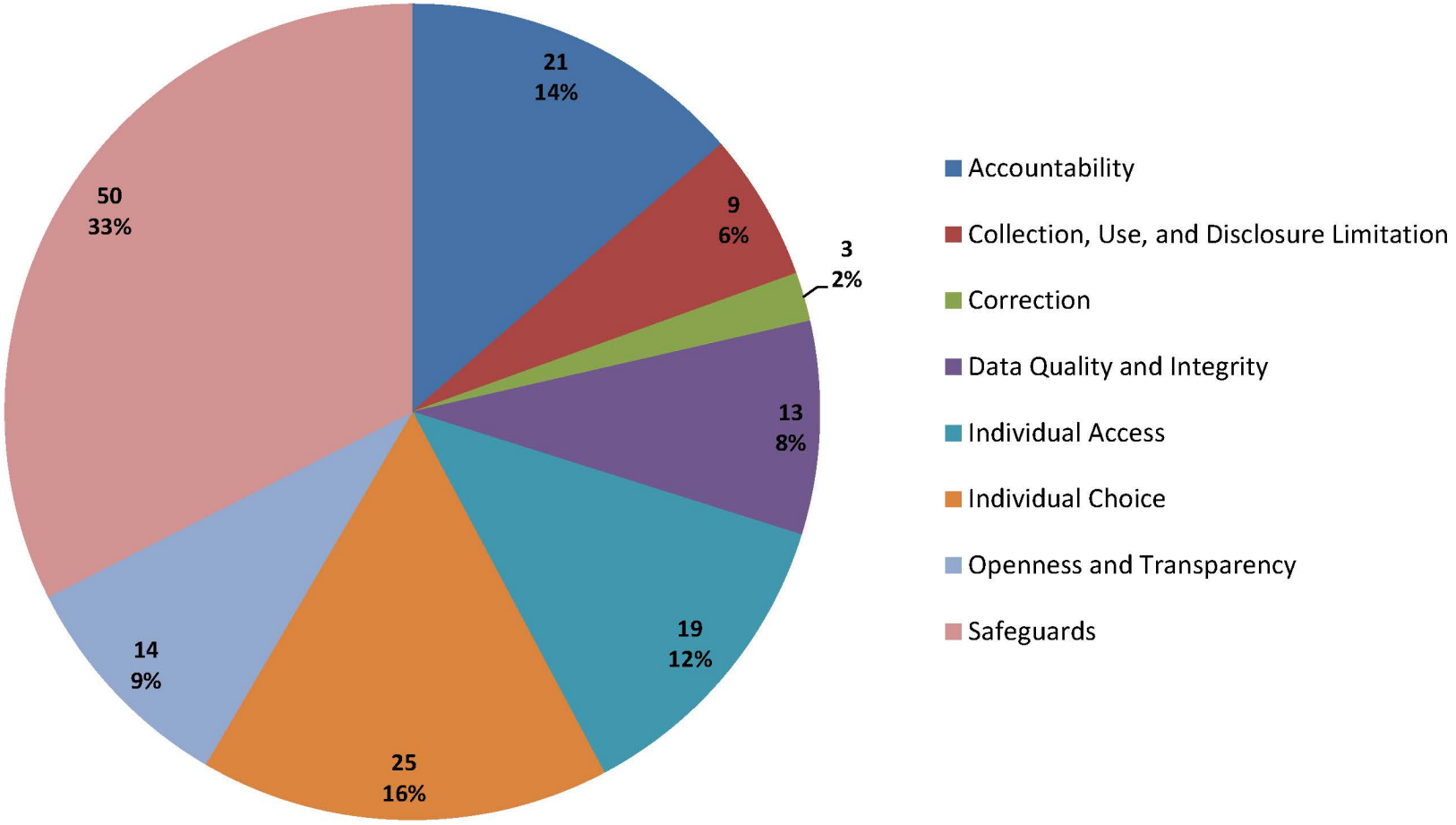
154 Recommendations Transmitted to ONC



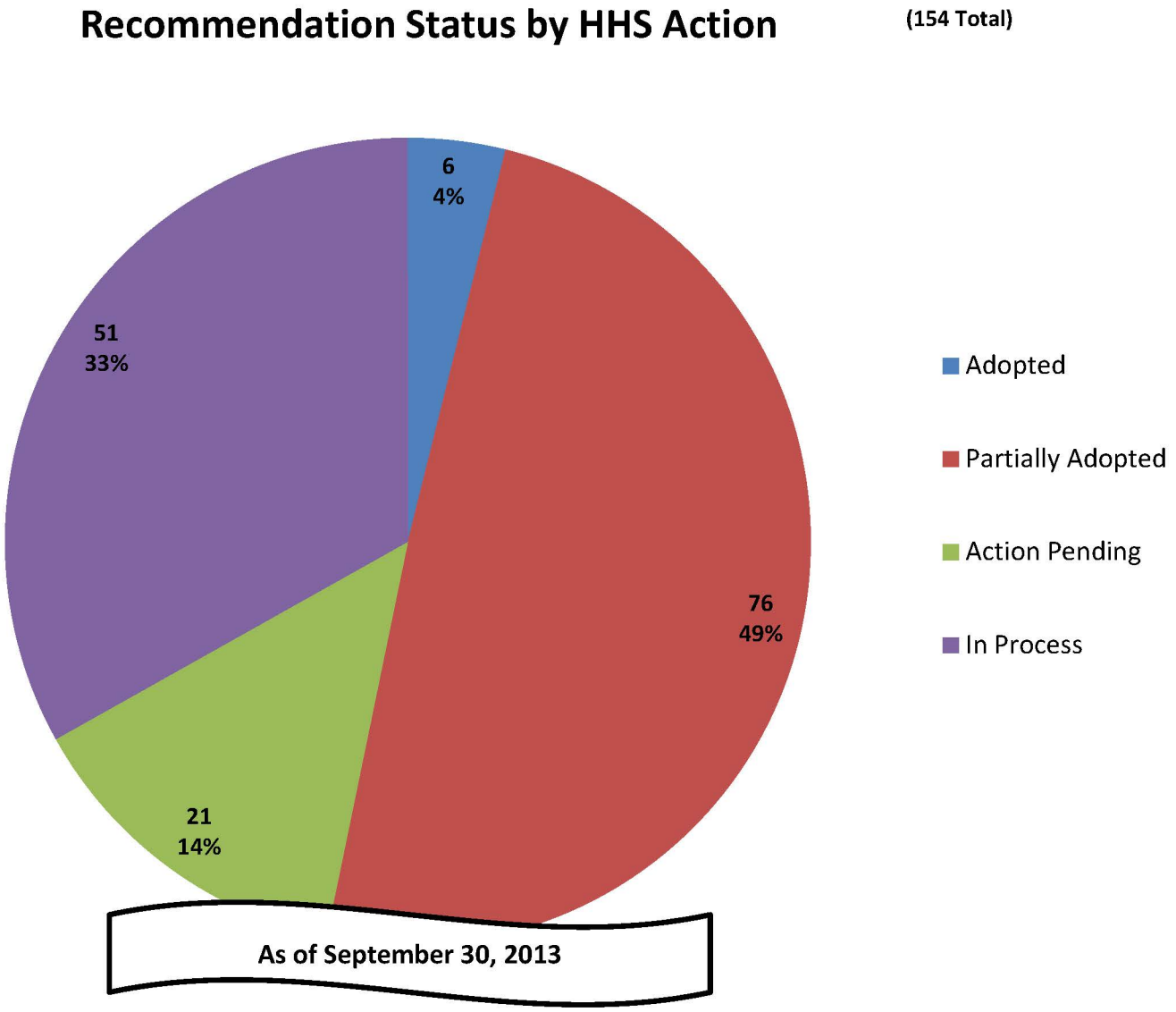
Recommendations Rooted in FIPPs

Recommendations by ONC Privacy and Security Principle

(154 Total)



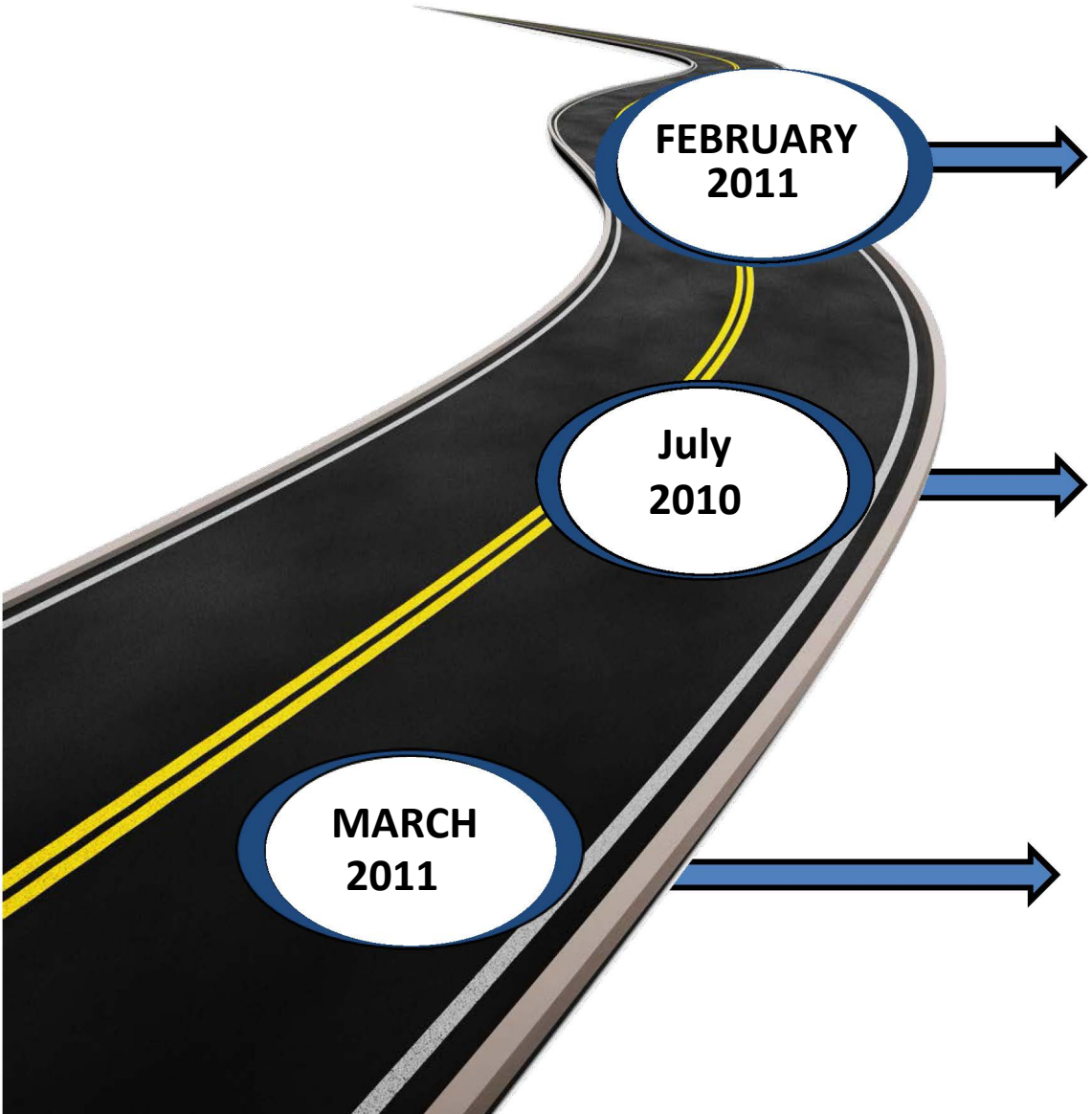
ONC Adopted over 50% of Recommendations



Recommendations Influenced Rulemaking Process

- Meaningful Use Stage 1: ONC and CMS
- Meaningful Use Stage 2: ONC and CMS
- Meaningful Use Stage 3 Request for Comment
- Clinical Laboratory Improvement Amendments (CLIA)
- The Common Rule Advanced Notice of Proposed Rulemaking (ANPRM)
- Recommendations also inform the Office of the Chief Privacy Officer (OCPO) comments on proposed federal rulemaking during the clearance process

HITPC Recommendation: Sample Implementation in Policy and Technical Assistance



ONC releases Security Risk Assessment Tool to Regional Extension Centers (RECs) providing technical assistance to professionals.

HHS releases final MU Stage 1 Rule requiring professionals and hospitals to attest to conducting or reviewing security risk assessment in order to receive payment.

HITPC recommendation: Include in MU Stage 1 requirement that eligible professionals and hospitals conduct a security risk assessment under HIPAA. ONC should provide appropriate guidance.

Recommendations Influenced ONC Program Guidance

- **Program Guidance examples include:**
  - State Health Information Exchange (HIE) – Program Information Notice (PIN) – 002: Requirements and Recommendations
  - HIE – PIN – 003: Privacy and Security Framework Requirements

ONC Projects Influenced by Recommendations

- Data Segmentation for Privacy (DS4P)*
- eConsent Trial Project*
- Mobile Device Provider Education
- Notice of Privacy Practices (NPP) Project*
- Provider and Staff Security Video Games*
- mHealth Consumer/Patient Research
- Exemplar Health Information Exchange Governance Entities Program (Program) Funding Opportunity
- The Query Health Initiative
- The Direct Project
- Blue Button FAQs*
- Data Provenance
- Patient Matching Initiative

*Indicates project was initiated in direct response to Tiger Team recommendations.


Office of the Chief Privacy Officer
The Office of the National Coordinator for
Health Information Technology


HealthIT.gov

FIPPs

- **Individual Access –** Individuals should be provided with a simple and timely means to access and obtain their health information in a readable form and format
- **Correction –** Individuals should be provided with a means to dispute the accuracy or integrity of their individually identifiable health information and to have erroneous information corrected or to have a dispute documented if their requests are denied
- **Openness and Transparency –** There should be openness and transparency about policies, procedures and technologies that directly affect individuals and/or their individually identifiable health information
- **Individual Choice –** Individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use and disclosure of their individually identifiable Health Information
- **Collection, Use and Disclosure Limitations –** Individually identifiable health information should be collected, used and/or disclosed only to the extent necessary to accomplish a specified purpose(s) and never to discriminate inappropriately
- **Data Quality and Integrity –** Persons and entities should take reasonable steps to ensure that individually identifiable health information is complete, accurate and up-to-date to the extent necessary for the person's or entity's intended purposes and has not been altered or destroyed in an unauthorized manner
- **Safeguards –** Individually identifiable health information should be protected with reasonable administrative, technical and physical safeguards to ensure its confidentiality, integrity, and availability, and to prevent unauthorized or inappropriate access, use, or disclosure
- **Accountability –** These principles should be implemented, and adherence assured, through appropriate monitoring and other means and methods should be in place to report and mitigate non-adherence and breaches

*The Tiger Team used the formulation of the Fair Information Practice Principles (FIPPs) endorsed by the HIT Policy Committee and adopted by ONC in the *Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information.*
http://www.healthit.gov/sites/default/files/nationwide-ps-framework-5.pdf