

## Policy Framework - Analysis of Gaps (January 31, 2011)

The Tiger Team has largely focused their recommendations on the uses and disclosures of information required for Stage 1 Meaningful Use (MU). Tiger Team will also need to apply the principles to additional uses and disclosures required for Stages 2 and 3 and other initiatives.

Policy Framework		
Policy principle	Definition	TT work to date/Gap analysis
Individual Access	Individuals should be provided with a simple and timely means to access and obtain their individually identifiable health information in a readable form and format.	In process: Patient access issues (including identity proofing and authentication) scheduled for 1Q 2011
Correction	Individuals should be provided with a timely 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.	Patient's ability to correct record – to be discussed by Tiger Team within overall “corrections” category [perhaps 2Q 2011?]
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.	Recommendations submitted on 10-20-2010 <i>Source: <a href="#">Privacy &amp; Security Tiger Team Recommendation on Transparency</a>.</i> Gap: Right of individuals to see who has accessed their information or to see an accounting of disclosures
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.	Recommendations submitted on 08-19-2010 <i>Source: <a href="#">Privacy &amp; Security Tiger Team Recommendations</a></i> <b>Gap:</b> choice with respect to access, use and disclosure beyond Stage 1
Collection, Use and Disclosure Limitation	Individually identifiable health information should be collected, used, and/or disclosed only to the extent necessary to accomplish a specified lawful purpose(s) and never to discriminate inappropriately.	Recommendations submitted on 08-19-2010 <i>Source: <a href="#">Privacy &amp; Security Tiger Team Recommendations</a></i> <b>Gap:</b> De-identified data; accountability for business associates
Data Integrity and Quality	Persons and entities should take reasonable steps to ensure that individually identifiable health	In process: Patient matching

## Policy Framework

Policy principle	Definition	TT work to date/Gap analysis
	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.	<b>Gap:</b> Propagation of corrections by providers, data accuracy & completeness beyond matching?
Safeguards <sup>1</sup>	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.	<p>Provider-entity authentication recommendations submitted 11/19/10; User authentication planned for 1Q 2011</p> <p><b>Gap:</b> Use of tools in certified EHRs (Privacy &amp; Security workgroup recommended meaningful users have a plan to address as part of Stage 1 – but not adopted by CMS); encryption &amp; access controls (for ex., approach recommended in PCAST); note assumptions made in Tiger Team August recommendations ensured a baseline level of security. A general list of other security safeguards that may be considered includes, but is not limited to the following:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Access controls (e.g., role-based access)</li> <li><input type="checkbox"/> Network security (e.g., firewall, intrusion detection, and routing security) and antivirus/antimalware and vulnerability assessments (e.g., system penetration testing)</li> <li><input type="checkbox"/> Cryptography/encryption of data in-transit (e.g., across private, public and wireless networks) and at-rest for all devices and media (e.g., servers, desktops, laptops, external drives, mobile/smart phones)</li> <li><input type="checkbox"/> Monitoring and logging capabilities (e.g., traceability for audit and compliance requirements)</li> <li><input type="checkbox"/> Physical security (e.g., secure facility, etc.)</li> <li><input type="checkbox"/> Destruction/disposal of data</li> </ul>
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.	<p>Recommendations from the Governance workgroup established a process for establishing an accountability infrastructure for assuring adherence to a framework of privacy and security practices and policies; recommendations submitted on provider entity authentication November 2010</p> <p><b>Gap:</b> review previous recommendations for accountability/enforcement; follow-up on Governance work on Conditions of Trust &amp; Interoperability?</p>

<sup>1</sup> The specifications and requirements of the HIPAA Privacy and Security Rules should be taken in consideration for determining which Safeguards proposed topics be included in the P&S TT agenda

**Privacy and Security Tiger Team  
1Q 2011 Meeting Schedule and Agenda Planner**

<b>2011 Date</b>	<b>Time</b>	<b>Type of Meeting</b>	<b>Agenda</b>
1/4	2-4 pm	Tiger Team	<ul style="list-style-type: none"> <li>• Patient matching recommendations</li> </ul>
1/5	10 am – 3 pm	HIT Policy Committee	
1/18	2-4 pm	Tiger Team	<ul style="list-style-type: none"> <li>• Continue patient matching recommendations if needed</li> </ul>
2/2	10 am – 3 pm	HIT Policy Committee	Present patient matching recommendations
2/4	10 -12 am	Tiger Team	<ul style="list-style-type: none"> <li>• Debrief 2/2 Policy Committee meeting</li> <li>• Review PCAST report recommendations relevant to TT</li> <li>• Introduce Framework Gap Analysis on Proposed Meeting Planner for Q1</li> <li>• Begin user authentication</li> </ul>
2/14	10 -12 am	Tiger Team	<ul style="list-style-type: none"> <li>• User authentication</li> </ul>
2/25	10 – 12 pm	Tiger Team	<ul style="list-style-type: none"> <li>• Wrap up User authentication</li> <li>• Begin Patient access (including identity proofing and authentication)</li> </ul>
3/2	10 am -3 pm	HIT Policy Committee	Present user authentication recommendations
3/7	10 – 12 pm	Tiger Team	<ul style="list-style-type: none"> <li>• Patient access (including identity proofing and authentication )</li> </ul>
3/23	2-4 pm	Tiger Team	<ul style="list-style-type: none"> <li>• Patient access (including identity proofing and authentication )</li> </ul>
4/13	10 am -3 pm	HIT Policy Committee	Present patient access recommendations