



## **HITECH Risk Assessment Starter Kit**

### **PREVIEW PAGES**

**The following pages include excerpts and samples derived directly from the HyperionGP *HITECH Risk Assessment Starter Kit*. This preview document is prepared to be representative of the materials you will receive with your purchase of the Starter Kit.**





# HITECH RISK ASSESSMENT

## STARTER KIT

### *Overview*

In February 2010, the US Congress enacted the Health Information Technology for Economic and Clinical Health (HITECH) Act. As a result, law firms, acting as Business Associates for their clients with whom they exchange Protected Health Information, are now required to be HIPAA compliant. Simply put, under the Core Regulations the Business Associate must:

- Ensure the confidentiality, integrity, and availability of all electronic protected health information (“ePHI”) the Business Associate creates, receives, maintains, or transmits;
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the HIPAA Privacy Regulations; and
- Ensure compliance with the HIPAA Security Regulations by its workforce.

**The first requirement of the new law is to complete a risk assessment to determine your firm's current level of compliance.**

Not only is it a government requirement, it is also the most efficient means of understanding the privacy/security landscape within your Firm. The risk assessment process is critical to formulating a deep understanding of when, where and how protected health information (“PHI”) moves throughout your organization. **If you do not understand the location of and movement of Protected Health Information across your Firm, you cannot ensure mitigation all of the potential risks that PHI is at for loss or inappropriate disclosure.**





## Starter Kit Description

The **HGP HITECH Risk Assessment Starter Kit** is designed to give you everything you need to complete a thorough analysis of your Firm’s privacy and security landscape. The Starter Kit Contains six component documents, described as follows:

Document Description and Overview		
1.	<b>Getting Started</b>	Overview of Starter Kit and steps for getting started
2.	<b>Risk Assessment Project Plan</b>	Sample project plan, including assumptions regarding <ol style="list-style-type: none"> <li>a. How long the project may take</li> <li>b. Who should complete the steps</li> </ol>
3.	<b>Compliance Team</b>	Includes information required to establish your Firm’s Compliance Team <ol style="list-style-type: none"> <li>a. Team membership</li> <li>b. Team roles and responsibilities</li> </ol>
4.	<b>End user Interview Guides</b>	<ol style="list-style-type: none"> <li>1. Instructions for setting up and facilitating the interviews</li> <li>2. Sample Interview Guides for Practitioners, Administration and Information Technology</li> </ol>
5.	<b>Facilitator Interview Guides</b>	<ol style="list-style-type: none"> <li>1. Facilitator Interview Guides/Survey Template for taking notes during the interview, or for use as a survey</li> <li>2. Delivered in MS Word 2007 format to allow updating</li> </ol>
6.	<b>Risk Matrix by Safeguard and Implementation Specification</b>	<ol style="list-style-type: none"> <li>1. Contains the actual HIPAA Security Rule requirements outlining exactly what steps your Firm must take to get into compliance.</li> <li>2. The matrix is organized by safeguard and implementation specification to ensure a complete and accurate evaluation:                             <ol style="list-style-type: none"> <li>a. Administrative, Technical, Physical, Organization/Policy/Process Safeguards                                     <ul style="list-style-type: none"> <li>– Each Safeguard is supported by <b>Implementation Specifications</b>, which are intended to give more specific instruction on “what” to do</li> </ul> </li> <li>b. This document also addresses developing the long-term implementation strategy</li> </ol> </li> <li>3. Delivered in MS Word 2007 format to allow updating</li> </ol>

Each document contains an “**Instructions for Use**” initiating section, clearly outlining the use, responsibility and intended audience for each document and/or form contained within the document.



## *One-on-one Assistance*

Purchase of the Starter Kit also provides you up to 1.5 hours of consulting during project kickoff with a Hyperion Compliance Expert. We will guide you through the assessment process as follows:

- Description of all documents and how/when to use them
- How to perform the interviews
- What type of information to gather and how to document interview notes
- Discuss the Risk Matrix and how to use it when documenting the current state
- How to develop the implementation strategy





End User Interview Guides

END USER INTERVIEW GUIDES	
Instructions for Use	
<b>Overview and Use</b>	<p>This document provides guidance on scheduling, managing and performing the risk assessment end user interviews. Should your Firm choose to complete an information gathering survey instead of interviews; those instructions are included as well.</p> <p>This document contains the following forms:</p> <ul style="list-style-type: none"> <li>Practitioner, Administrative and Information Technology End User Interview Guides</li> </ul> <p>This document should be used in conjunction with <b>Document Five: Facilitator Interview Guide/Survey Template</b>, which is used to document notes during the meetings</p>
<b>Responsible Party(ies) and Intended Audience</b>	<p><b>Interviews</b></p> <ul style="list-style-type: none"> <li>The Interview Facilitator will use the steps outlined in this document to schedule and manage the interview process</li> <li>The Interview Facilitator will send out the end user interview guides in this document to all interviewees prior to the meeting to inform interviewees on what to expect during the interviews</li> <li>The Interview Facilitator will then use the <b>Facilitator Interview Guide/Survey Template in Document Five</b> to capture notes during interviews                         <ul style="list-style-type: none"> <li>If the Firm will survey instead of interview, the project owner will use as the <b>Facilitator Interview Guide/Survey Template in Document Five</b> as a survey to gather information</li> </ul> </li> </ul>
<b>Duration</b>	<p>Assume two weeks to complete from scheduling the meetings to compiling your notes. If you choose to perform a survey instead, assume two-three weeks.</p>

**Contents**

Interview Guides and Strategies ..... 2

    Managing the Interview Process..... 3

    Survey Process ..... 5

Practitioner Interview Guide..... 6

Administrative Interview Guide ..... 7

Information Technology Interview Guide ..... 9





## Example Risk Matrix

Following is an example of the Risk Matrix, along with an explanation of each row/column. Please carefully review this before moving on to the actual Risk Matrix.

IDENTIFIES SPECIFICATION AS REQUIRED OR ADDRESSABLE

DOCUMENT WHAT THE FIRMS CURRENT LEVEL OF COMPLIANCE REGARDING THIS IMPLEMENTATION SPECIFICATION

REQD/ADD	ITEM # TASK	DHHS DESCRIPTION	CURRENT STATUS	TASKS REQUIRED
<b>Administrative Safeguards</b> <i>Administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information.</i>				
<b>Security Management Process</b> <i>"Implement policies and procedures to prevent, detect, contain and correct security violations."</i>				
Required	<b>1</b> <i>Risk assessment</i>	<i>Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.</i>	<ul style="list-style-type: none"> <li>The firm is undergoing a formal risk assessment in the healthcare , medical malpractice and product liability group</li> </ul>	<ul style="list-style-type: none"> <li>Update risk assessment as technology or practices are added or rules change</li> <li>Establish policy to complete formal risk assessment yearly</li> </ul>
Required	<b>2</b> <i>Risk Management</i>	<i>Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a).</i>	<b>EXAMPLE ANSWER</b> <ul style="list-style-type: none"> <li>Ongoing as new technologies are added</li> <li>Implemented per findings in risk assessment</li> </ul>	<b>EXAMPLE TASKS</b> <ul style="list-style-type: none"> <li>Complete all mitigation steps as outlined in the risk assessment</li> </ul>
Required	<b>3</b> <i>Sanction Policy</i>	<i>Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.</i>	<b>EXAMPLE ANSWER</b> <ul style="list-style-type: none"> <li>Sanction verbiage exists in the current Information Security Policy:</li> <li>"Attempts to violate the provisions of this policy will result in disciplinary action ranging from the temporary revocation of user access to termination of employment"</li> <li>The existing sanction verbiage is compliant with the Security Rule. However, the memo signed by employees only addresses email and internet usage.</li> </ul>	<b>EXAMPLE TASKS</b> <ul style="list-style-type: none"> <li>Create additional, or update existing Information Security Policies to specifically address privacy and security of PII and PHI, for all client records, electronic or not.</li> <li>Add definition of PII and PHI to all relevant policies.</li> </ul>

IMPLEMENTATION SPECIFICATION GENERAL CATEGORY

HIPAA SECURITY RULE IMPLEMENTATION SPECIFICATION VERBIAGE FROM THE DEPT. OF HEALTH AND HUMAN SERVICES

THE TASKS THAT MUST BE COMPLETED BY THE FIRM TO ENSURE COMPLIANCE

