EHR 2.0
Ensure HIPAA Compliance

HIPAA/HITECH Compliance Assessment

EHR 2.0
Ensure HIPAA Compliance

Content

1. Company Background
2. Project Objectives and Overview
3. Options
4. Online Portal Capabilities
5. Proposed Process
6. Next Steps

EHR 2.0
Ensure HIPAA Compliance

EHR 2.0 Mission

To assist healthcare organizations and business associates to develop and implement practices to secure IT systems and comply with HIPAA/HITECH regulations and MIPS program.

EHR 2.0
Ensure HIPAA Compliance

Project Objectives

✓ Assessing the risk of patient data and deployment of on-premise applications

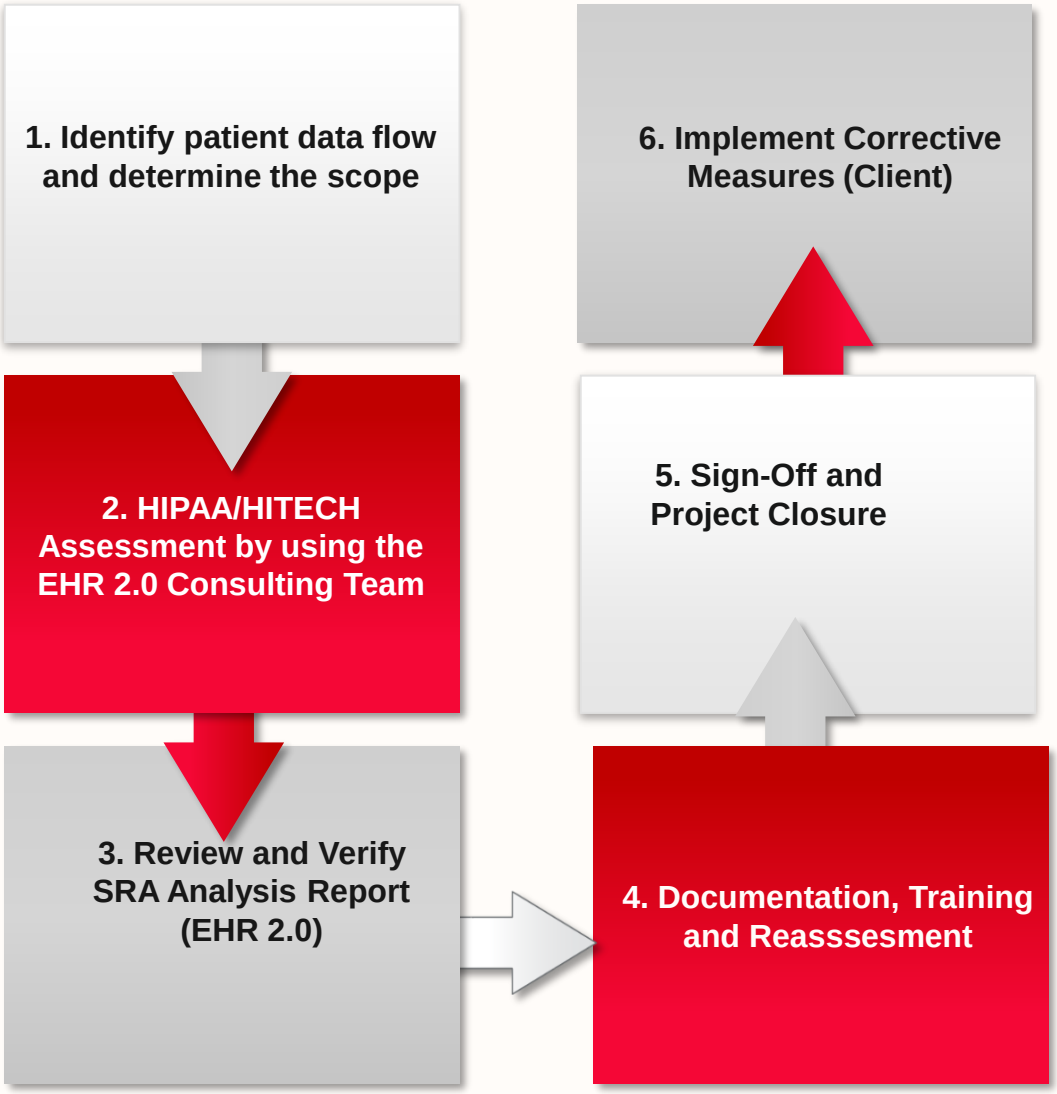
✓ Perform a risk assessment and assess the compliance of patient data services and implementation of different services

✓ Identifying responsibilities and controls for applications

✓ Understand available controls on how to implement and configure them to manage security and compliance with applicable regulatory requirements especially HIPAA/HITECH

✓ Offering implementation guidance to help accomplish the business objectives, tasks and better manage the risks

Proposed Security Risk Analysis Process



Deliverables

- ✓ ePHI Inventory Sheet
  - ✓ Scoping and Profiling
- ✓ Security Risk Analysis Report
  - ✓ Vulnerability assessment
- ✓ HIPAA/HITECH Assessment Report
- ✓ Risk Management Plan
- ✓ Customized Policies and Procedures
- ✓ Online User Training
- ✓ Executive Summary Report
- ✓ Portal Access

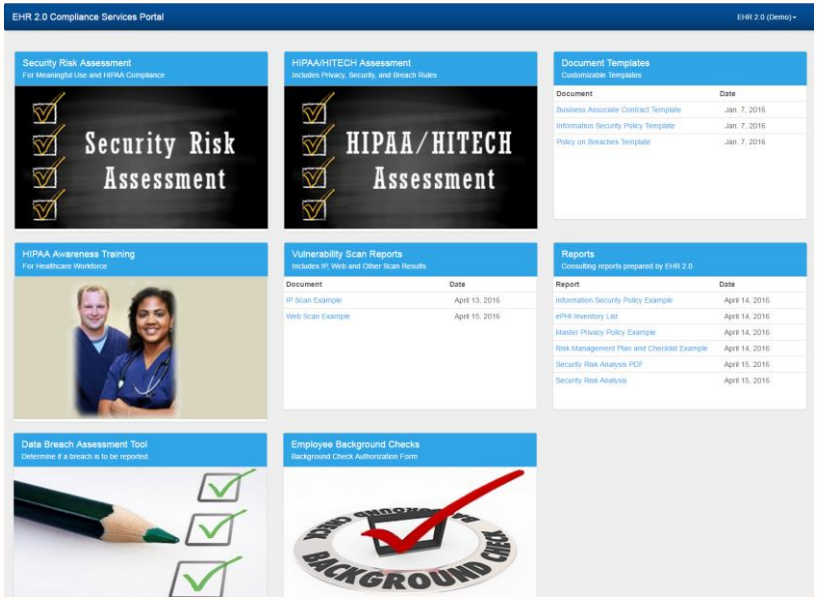
Audit Support Guarantee

We provide audit support/guarantee for all our consulting customers

EHR 2.0
Ensure HIPAA Compliance

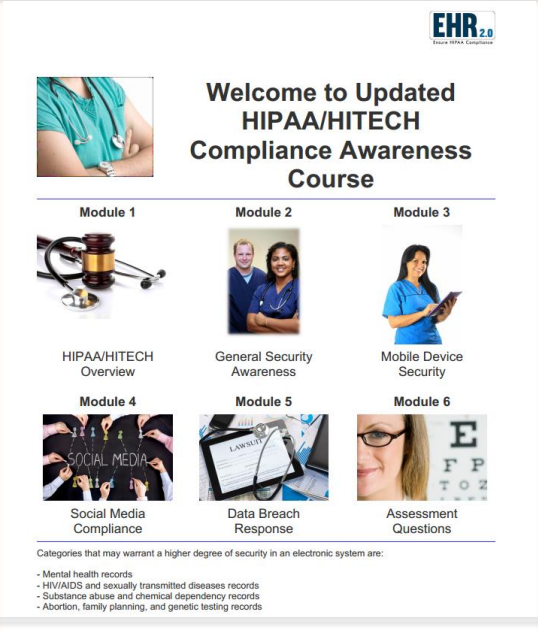
Online Portal to Manage Deliverables

Packaged in one container



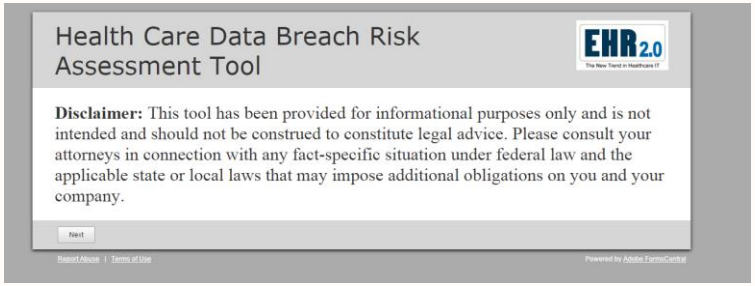
- Simple and easy to use web-based tool
- Covers HIPAA Security and Data breach requirements
- Content continuously updated to include new requirements
- Pre-populated solutions to track exposures, prioritize security risks, develop mitigation plan
- Continuously evaluate and update plans
- Download, print and/or store reports in portal

Online Portal to Manage Deliverables… Contd.



Online Security Awareness Training for Staff

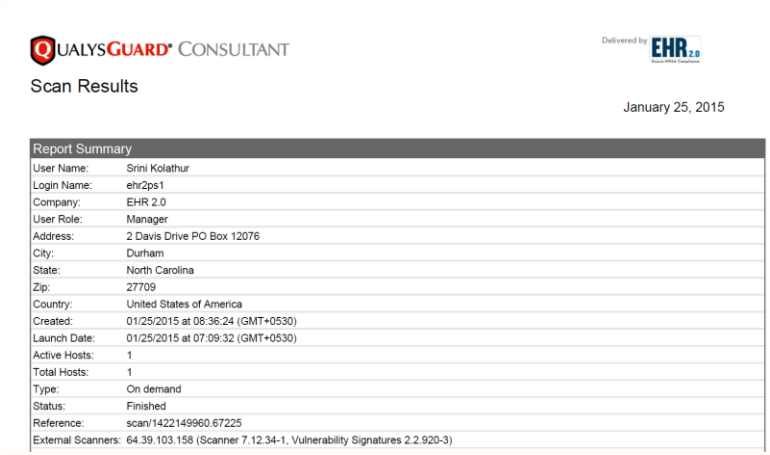
- 6 Modules
- Training log
- Customizable



Online Data Breach Risk Determination Tool

- Supports HITECH Data Breach Act
- Required documentation

Online Portal to Manage Deliverables… Contd.



QUALYSGUARD® CONSULTANT

Delivered by EHR 2.0

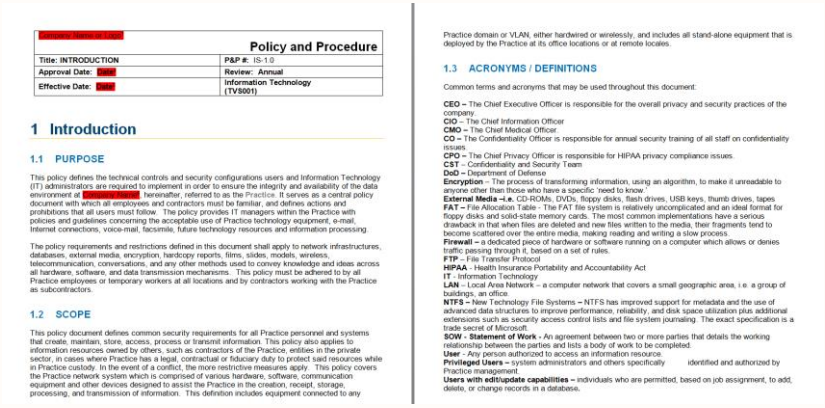
Scan Results

January 25, 2015

Report Summary	
User Name:	Srini Kolathur
Login Name:	ehr2ps1
Company:	EHR 2.0
User Role:	Manager
Address:	2 Davis Drive PO Box 12076
City:	Durham
State:	North Carolina
Zip:	27709
Country:	United States of America
Created:	01/25/2015 at 08:36:24 (GMT+0530)
Launch Date:	01/25/2015 at 07:09:32 (GMT+0530)
Active Hosts:	1
Total Hosts:	1
Type:	On demand
Status:	Finished
Reference:	scan/1422149960.67225
External Scanners:	64.39.103.158 (Scanner 7.12.34-1, Vulnerability Signatures 2.2.920-3)

Qualys Vulnerability Assessment

- Scan your external facing network
- Prioritize Risks



Policy and Procedure

Title: INTRODUCTION	P&P #: IS-1.0
Approval Date:	Review: Annual
Effective Date:	Information Technology (TV$001)

1 Introduction

1.1 PURPOSE

This policy defines the technical controls and security configurations users and Information Technology (IT) administrators are required to implement in order to ensure the integrity and availability of the data environment of [redacted] hereinafter, referred to as the Practice. It serves as a central policy document with which all employees and contractors must be familiar, and defines actions and prohibitions that all users must follow. The policy provides IT managers within the Practice with policies and guidelines concerning the acceptable use of Practice technology equipment, e-mail, Internet connections, voice-mail, facsimile, future technology resources and information processing.

The policy requirements and restrictions defined in this document shall apply to network infrastructures, databases, external media, encryption, hardcopy reports, films, slides, models, wireless, telecommunication, conversations, and any other methods used to convey knowledge and ideas across all hardware, software, and data transmission mechanisms. This policy must be adhered to by all Practice employees or temporary workers at all locations and by contractors working with the Practice as subcontractors.

1.2 SCOPE

This policy document defines common security requirements for all Practice personnel and systems that create, maintain, store, access, process or transmit information. This policy also applies to information resources owned by others, such as contractors of the Practice, entities in the private sector, in cases where Practice has a legal, contractual or fiduciary duty to protect said resources while in Practice custody. In the event of a conflict, the more restrictive measures apply. This policy covers the Practice network system which is comprised of various hardware, software, communication equipment and other devices designed to assist the Practice in the creation, receipt, storage, processing, and transmission of information. This definition includes equipment connected to any Practice domain or VLAN, either hardwired or wirelessly, and includes all stand-alone equipment that is deployed by the Practice at its office locations or at remote locales.

1.3 ACRONYMS / DEFINITIONS

Common terms and acronyms that may be used throughout this document:

CEO – The Chief Executive Officer is responsible for the overall privacy and security practices of the company.
CIO – The Chief Information Officer
CMO – The Chief Medical Officer
CO – The Confidentiality Officer is responsible for annual security training of all staff on confidentiality issues.
CPO – The Chief Privacy Officer is responsible for HIPAA privacy compliance issues.
CST – Confidentiality and Security Team
DoD – Department of Defense
Encryption – The process of transforming information, using an algorithm, to make it unreadable to anyone other than those who have a specific 'need to know.'
External Media –i.e. CD-ROMs, DVDs, floppy disks, flash drives, USB keys, thumb drives, tapes.
FAT – File Allocation Table - The FAT file system is relatively uncomplicated and an ideal format for floppy disks and solid-state memory cards. The most common implementations have a serious drawback in that when files are deleted and new files written to the media, their fragments tend to become scattered over the entire media, making reading and writing a slow process.
Firewall – a dedicated piece of hardware or software running on a computer which allows or denies traffic passing through it, based on a set of rules.
FTP – File Transfer Protocol
HIPAA - Health Insurance Portability and Accountability Act
IT - Information Technology
LAN – Local Area Network – a computer network that covers a small geographic area, i.e. a group of buildings, an office
NTFS – New Technology File Systems – NTFS has improved support for metadata and the use of advanced data structures to improve performance, reliability, and disk space utilization plus additional extensions such as security access control lists and file system journaling. The exact specification is a trade secret of Microsoft.
SOW - Statement of Work - An agreement between two or more parties that details the working relationship between the parties and lists a body of work to be completed.
User - Any person authorized to access an information resource.
Privileged Users – system administrators and others specifically identified and authorized by Practice management.
Users with edit/update capabilities – individuals who are permitted, based on job assignment, to add, delete, or change records in a database.

Customized Policies and Procedures

- Covers all key policy areas
- Security and Breach Policies

EHR 2.0
Ensure HIPAA Compliance

Next Steps

1. Review proposal
2. Questions, concerns and feedback
3. Finalize purchase order
4. Schedule initial calls with the technical team
5. Project plan and deliverable timeline will be shared upon further discussion
6. Portal setup and schedule training for consultants

Contact Us

E-mail: info@ehr20.com

Phone: 1-866-276 8309

THANK YOU!