

# HIPAA/HITRUST FastTrack Toolkit



**+80** policy and procedure documents

**+480** pages of comprehensive details

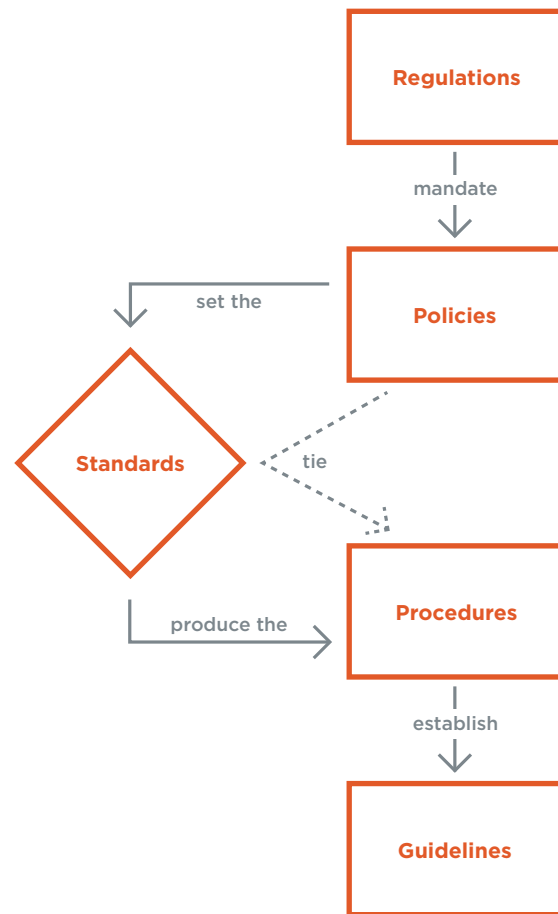
There is often a misconception that regulations, policies, procedures, standards, and guidelines are interchangeable or synonymous with each other. This could not be further from the truth. To understand the differences, these terms need to be fully explained as they relate to compliance and defined as they relate to HIPAA and HITRUST CSF.

HIPAA is legislation composed of regulations that are legally mandated. These regulations must be implemented and compliance must be met or there could be severe consequences. *Regulations* form the basis for a covered entity’s policies. *Policies* are the intentions of the organization’s management to comply with the regulations. Policies are documented, high-level requirements that are approved by management to provide direction for employees in the process of complying with the stated objectives.

Policies set the *standards* that help produce the *procedures* that will be followed to carry out the policies’ objectives. Standards attempt to tie the procedures with the associated policies. Procedures are more detailed than policies and normally provide step-by-step instructions for complying with the policy.

Typically, a covered entity has one policy statement and several procedures that explain what should be done to carry out the policy. Once procedures have been developed, *guidelines* are usually established. Guidelines are common practices that are followed by employees of a covered entity and are usually the “real-life” practices that are established by a given procedure.

The diagram provides a view of how regulations, policies, procedures, standards, and guidelines work together.



**Each policy contains:**

- Purpose
- Policy statement
- Background/definitions
- Standards
- Implementation procedures
- Reporting/documentation
- References

## FAST TRACK TOOLKIT CONTENT

Acceptable Use Policy	Access Agreement	Access Authorization Policy	Access Control Policy
Access Encryption and Decryption Policy	Access Establishment and Modification Policy	Administrative Safeguards Policy	Application Development
Applications and Data Criticality Analysis Policy	Assigned Privacy/Security Responsibility Policy	Auditing and Logging Control Policy	Authorization and/or Supervision Policy
Automatic Logoff Policy	Business Associate Contract Obligations Policy (Third-party Agreements)	Change Management Policy (Configuration Management)	Clear Desk Policy
Compliance Policy	Contingency Planning Policy	Data Backup Policy	Device and Mobile Media Controls Policy
Disaster Recovery Policy	Email Retention Policy	Email/Phone Policy	Emergency Access Policy
Emergency Mode Operations Policy	Evaluation/Vulnerability/ Penetration Test Policy	Exception Management Policy	Facility Access Controls Policy
Facility Security Policy	Facsimile Machine Policy	Firewall Management	Guidelines for Media Sanitization and Secure Disposal
Full Incident Response Plan	Information Access Management Policy	Information Handling	Information Security Management Policy
Information System Activity Review Policy	Integrity Policy	Internet Use Policy	Log Monitoring Policy
Asset Maintenance Records Policy (Maintenance and Repair)	Malicious Software Management and Malware Protection Policy	Mechanism to Authenticate Policy	Media Sanitization Validation Form
Mobile Device Acknowledgement and Agreement Form	Mobile Device/BYOD Policy	Network Management	Out-of-bounds/Secondary Level of Authentication
Policies/Procedures Overview	Password Management Policy	Person or Entity Authentication Policy	Personnel Security Policy
Physical Access Control and Validation Policy	Physical Contingency Operations Policy	Physical Safeguard and Environmental Security Policy	Remote Access Policy
Request for Exception Form	Risk Analysis Policy	Risk Management Policy	Sample Business Associate Agreement Provisions
Sanction Policy	Security Awareness Training Policy	Security Incident Response and Reporting Policy	Security Management/ Risk Assessment Policy (Asset Management)
Security Reminders Policy	Social Media Policy	System Boundaries Examples	Technical Safeguard Policy
Teleworking	Termination Policy	Testing and Revision Policy	Transmission Encryption Policy
Transmission Integrity Control Policy	Transmission Security Policy	Unique User Identification Policy	Vendor Due Diligence Policy (Third-party Security)
Vendor Due Diligence Policy (Third-party Service Delivery)	Full Vendor Management Program	Visitor Security Policy	Vulnerability Management Policy
Wireless Access and Security Policy	Workforce Clearance Policy	Workforce Security Policy	Workstation Use and Security Policy

## COVERS ALL HIPAA SECURITY RULE REQUIREMENTS AND 19 HITRUST CSF DOMAINS

<b>01</b> Information Protection Program	<b>11</b> Access Control
<b>02</b> Endpoint Protection	<b>12</b> Audit Logging and Monitoring
<b>03</b> Portable Media Security	<b>13</b> Education, Training, and Awareness
<b>04</b> Mobile Device Security	<b>14</b> Third-party Assurance
<b>05</b> Wireless Security	<b>15</b> Incident Management
<b>06</b> Configuration Management	<b>16</b> Business Continuity and Disaster Recovery
<b>07</b> Vulnerability Management	<b>17</b> Risk Management
<b>08</b> Network Protection	<b>18</b> Physical and Environmental Security
<b>09</b> Transmission Protection	<b>19</b> Privacy
<b>10</b> Password Management	

In addition, our [CoalfireOne<sup>sm</sup> platform](#) provides organizations with the testing, documentation, reporting tools, and QSA support needed to support all of your HIPAA/HITRUST compliance needs. The easy-to-use and secure CoalfireOne platform contains advanced features that make managing your risk and compliance program much easier.

DS\_FastTrackToolkit\_052617

IMPROVE THE EFFECTIVENESS OF  
CYBER RISK AND SECURITY MANAGEMENT.

Learn more about Coalfire's Advisory Services.  
[Coalfire.com](http://Coalfire.com) | 877-224-8077

**COALFIRE**

### About Coalfire

As cybersecurity risk management and compliance experts, Coalfire delivers cybersecurity advice, assessments, testing, and implementation support to IT and security departments, executives, and corporate directors of leading enterprises and public sector organizations. By addressing each organization's specific challenges, we're able to develop a long-term strategy that improves our clients' overall cyber risk profiles. Armed with our trusted insights, clients can get to market faster with the security to succeed. Coalfire has offices throughout the United States and Europe. [Coalfire.com](http://Coalfire.com)

Copyright © 2014-2017 Coalfire Systems, Inc. All Rights Reserved. Coalfire is solely responsible for the contents of this document as of the date of publication. The contents of this document are subject to change at any time based on revisions to the applicable regulations and standards (HIPAA, PCI DSS et.al). Consequently, any forward-looking statements are not predictions and are subject to change without notice. While Coalfire has endeavored to ensure that the information contained in this document has been obtained from reliable sources, there may be regulatory, compliance, or other reasons that prevent us from doing so. Consequently, Coalfire is not responsible for any errors or omissions, or for the results obtained from the use of this information. Coalfire reserves the right to revise any or all of this document to reflect an accurate representation of the content relative to the current technology landscape. In order to maintain contextual accuracy of this document, all references to this document must explicitly reference the entirety of the document inclusive of the title and publication date; neither party will publish a press release referring to the other party or excerpting highlights from the document without prior written approval of the other party. If you have questions with regard to any legal or compliance matters referenced herein you should consult legal counsel, your security advisor and/or your relevant standard authority.