

# HIPAA Compliance Task List

## HIPAA Task List from regulations – minimum requirements

TASK DESCRIPTIONS BY TYPE	HIPAA Reg.	Other Legis.	Assigned to	Status
<b>HIPAA PRIVACY RULE</b>				
<b>I. Individual Rights/Communications</b>				
Notice of Privacy Practices <ul style="list-style-type: none"> <li>• Develop model notice(s)</li> <li>• P&amp;Ps for distributing notices</li> <li>• P&amp;Ps for acknowledgement(s)</li> <li>• P&amp;Ps for use of EDMS or other ways of tracking notices</li> <li>• Notice posted at provider sites as applicable</li> <li>• Procedure for distributing revised notices</li> <li>• Summary page (optional)</li> <li>• Non-English language use (not req'd by HIPAA, but need consistency)</li> </ul>	164.401(i); 164.520; 164.530(i)(4); 164.502(i)			
Document the “designated record set” <ul style="list-style-type: none"> <li>• Remember that minimum necessary applies here, too</li> <li>• Include fields we use in treatment, payment and operations</li> </ul>	164.501, 164.524, 164.526			
Individual Requests for PHI Access <ul style="list-style-type: none"> <li>• P&amp;P for handling requests</li> <li>• Request for Access form</li> <li>• Form letter for granting access</li> <li>• Form letter for denying access</li> <li>• Notice of time extension, if necessary</li> </ul>	164.524	note MGDPA timeframes		
Individual Requests to Amend PHI <ul style="list-style-type: none"> <li>• P&amp;P for handling requests</li> <li>• Form to request PHI amendment</li> <li>• Form letter to approve amendment</li> <li>• Form letter to deny amendment</li> <li>• Notice of time extension, if necessary</li> </ul>	164.526	note MGDPA timeframes		
Individual Requests for Accounting of Disclosures <ul style="list-style-type: none"> <li>• P&amp;P for tracking disclosures (which need to be tracked,</li> </ul>	164.528	note MGDPA timeframes		

# HIPAA Compliance Task List

TASK DESCRIPTIONS BY TYPE	HIPAA Reg.	Other Legis.	Assigned to	Status
which don't) <ul style="list-style-type: none"> <li>• P&amp;P for handing requests</li> <li>• Form to request an accounting</li> <li>• Format/specs for disclosure report</li> <li>• Notice of time extension, if necessary</li> </ul>				
Individual Requests for Restrictions on Uses/Disclosures or Alternative Communications <ul style="list-style-type: none"> <li>• P&amp;Ps for handling requests</li> <li>• Form for requesting restrictions or alternate communications</li> <li>• Form letter to approve request</li> <li>• Form letter to deny request</li> <li>• Flag on systems, in files, to alert</li> </ul>	164.502(c); 164.502(h); 164.522(a); 164.522(b)			
<b>II. Uses and Disclosures</b>				
Treatment, Payment, Health Care Operations <ul style="list-style-type: none"> <li>• P&amp;Ps for:                             <ul style="list-style-type: none"> <li>○ use/disclosure for payment</li> <li>○ use/disclosure for operations, including QA, training, audit</li> <li>○ use/disclosure for treatment, including emergency care</li> </ul> </li> <li>• Consent procedure (if req'd by State)</li> <li>• Consent forms (if req'd by State law)</li> </ul>	164.506			
Workforce access to records <ul style="list-style-type: none"> <li>• P&amp;P to define workforce</li> <li>• P&amp;P to define minimum necessary rule for various job functions</li> </ul>	164.501; 164.502(b); 164.514(d)			
Minimum Necessary Disclosure <ul style="list-style-type: none"> <li>• Routine / Recurring – Need protocols</li> <li>• Non-routine – criteria for determining minimum disclosure and process reviewing requests</li> </ul>	164.502(b); 164.514(d)			
Requesting PHI from another entity <ul style="list-style-type: none"> <li>• P&amp;P for requesting PHI</li> </ul>	164.508; 164.502(b);			

## HIPAA Compliance Task List

<b>TASK DESCRIPTIONS BY TYPE</b>	<b>HIPAA Reg.</b>	<b>Other Legis.</b>	<b>Assigned to</b>	<b>Status</b>
<ul style="list-style-type: none"> <li>Establishing minimum necessary criteria for various PHI requests</li> </ul>	164.514(d)			
Family / Caregivers <ul style="list-style-type: none"> <li>P&amp;Ps for uses and disclosures to family and caregivers (MGDPA etc.)</li> </ul>	164.510(a)			
Public Purposes <ul style="list-style-type: none"> <li>P&amp;Ps regarding uses &amp; disclosures:               <ul style="list-style-type: none"> <li>required by law</li> <li>for public health purposes</li> <li>disclosures of reports of abuse, neglect, domestic violence and endangerment</li> <li>Health Oversight Activities</li> <li>Responding to court /admin orders, subpoenas, discoveries</li> <li>Requests from law enforcement</li> <li>Averting threats to health/safety</li> </ul> </li> </ul>	164.512(a-f); 164.512(j)			
Deceased Individuals <ul style="list-style-type: none"> <li>P&amp;Ps for uses &amp; disclosures of PHI of deceased individuals, esp. re:               <ul style="list-style-type: none"> <li>Organ/tissue donations</li> <li>Coroners/Medical examiners</li> <li>Funeral directors</li> </ul> </li> </ul>	164.502(f-g); 164.512(g-h)			
Workers' Compensation <ul style="list-style-type: none"> <li>P&amp;Ps for uses and disclosures</li> </ul>	164.512(l)			
Parents / Personal Representatives <ul style="list-style-type: none"> <li>P&amp;P for designation of personal representative</li> </ul>	164.502(g)	State laws re: parental access		
Authorization <ul style="list-style-type: none"> <li>Checklist to determine whether authorization is required</li> <li>P&amp;Ps for giving and revoking auths</li> <li>Form to give individual authorization</li> <li>Form to revoke authorization</li> </ul>	164.508			
Incoming Authorizations <ul style="list-style-type: none"> <li>If external forms are accepted, develop checklist to determine HIPAA compliance of forms</li> </ul>	164.508			

# HIPAA Compliance Task List

<b>TASK DESCRIPTIONS BY TYPE</b>	<b>HIPAA Reg.</b>	<b>Other Legis.</b>	<b>Assigned to</b>	<b>Status</b>
Identification of Requester of PHI	164.514(h)			
Appropriate safeguards	164.530(c); 164.502(a)(1)(iii)			
Incidental Disclosures <ul style="list-style-type: none"> <li>• Policies to include appropriate safeguards and minimum necessary:                             <ul style="list-style-type: none"> <li>○ Identifying patients in a waiting area or room</li> <li>○ Registration/Scheduling</li> <li>○ Appointment reminders</li> <li>○ Whiteboard use</li> <li>○ Overhead paging</li> <li>○ Janitorial/maintenance staff</li> <li>○ Mailings or email to clients</li> <li>○ Oral communications, interviews</li> </ul> </li> </ul>	164.502(a)(1)(iii) 164.530(c) <i>[safeguards]</i> 164.514(d) <i>[minimum nec.]</i>			
Marketing <ul style="list-style-type: none"> <li>• P&amp;Ps for uses &amp; disclosures for marketing (define marketing)- needed for county?</li> <li>• Authorization form for marketing?</li> </ul>	164.514(f); 164.501 <i>[def. marketing];</i> 164.508			
Media <ul style="list-style-type: none"> <li>• Policy for disclosures to media</li> <li>• Authorization form</li> </ul>	164.508			
Fundraising (needed at county?) <ul style="list-style-type: none"> <li>• P&amp;Ps for Uses &amp; Disclosures</li> <li>• Authorization form (if needed)</li> <li>• Recordkeeping of opt-outs</li> </ul>	164.514(f)			
Mental Health Records <ul style="list-style-type: none"> <li>• P&amp;Ps for use, disclosure of MH records, incl. psychotherapy notes</li> <li>• Authorization form for psychotherapy notes</li> </ul>	164.508(1)	State laws		
Substance Abuse (CD) <ul style="list-style-type: none"> <li>• P&amp;Ps for uses and disclosures</li> </ul>	Part 2 of 42 CFR			
Other assorted uses and disclosures <ul style="list-style-type: none"> <li>• Disclosures to clergy</li> <li>• Disclosures to law enforcement</li> </ul>	164.510(b); 164.512(k)			

## HIPAA Compliance Task List

<b>TASK DESCRIPTIONS BY TYPE</b>	<b>HIPAA Reg.</b>	<b>Other Legis.</b>	<b>Assigned to</b>	<b>Status</b>
<ul style="list-style-type: none"> <li>• Disclosing admit/discharge information internally</li> <li>• Disclosures to military, armed forces</li> </ul>				
Research <ul style="list-style-type: none"> <li>• P&amp;Ps for use &amp; disclosures for research, including identification of potential subjects               <ul style="list-style-type: none"> <li>○ clinical research</li> <li>○ records research</li> <li>○ authorization forms</li> <li>○ documenting IRB waiver</li> </ul> </li> </ul>	164.512(i); 164.506; 164.508; 164.532			
Interns and Volunteers <ul style="list-style-type: none"> <li>• P&amp;Ps for use and disclosure by both interns and volunteers</li> <li>• P&amp;Ps for oversight and training</li> <li>• Confidentiality statements for non-Business Associates who have access to PHI</li> </ul>				
De-identification <ul style="list-style-type: none"> <li>• P&amp;Ps regarding how to de-identify data</li> <li>• P&amp;Ps regarding use and disclosure of de-identified data</li> </ul>	164.502(d); 164.514(a-c); 164.514(e)			
Limited Data Sets <ul style="list-style-type: none"> <li>• Policy for use of limited data sets</li> <li>• Procedures for creating limited data sets</li> <li>• Data Usage agreements</li> </ul>	164.502(d); 164.514(a-c); 164.514(e)			
<b>III. Business Associates</b>				
P&Ps for identifying Business Associates	164.502(e)			
Written Business Associate contracts	164.504(e)			
P&Ps for responding to Business Associate violations	164.532(d)			
<b>IV. Training Requirements</b>				
Training for entire workforce – HIPAA 101 (Ramsey County / DHS web-based training)	164.530(b)			
Advanced & targeted training to HIPAA-impacted departments	164.530(b)			
Forms/System to document training	164.530(b)			

# HIPAA Compliance Task List

<b>TASK DESCRIPTIONS BY TYPE</b>	<b>HIPAA Reg.</b>	<b>Other Legis.</b>	<b>Assigned to</b>	<b>Status</b>
Workforce confidentiality statements	164.530(b)			
<b>V. Administrative Tasks</b>				
Covered Entity Status <ul style="list-style-type: none"> <li>Apply definitions and make assessments to determine hybrid entity, covered entity, or affiliated</li> </ul>	164.504			
Compliance Code of Conduct – modify to incorporate privacy requirements	n/a			
Designation of Privacy Officer <ul style="list-style-type: none"> <li>Job Description</li> <li>RBA, Recommendation, Decision</li> </ul>	164.530(a)			
Designation of Contact Person / Office for questions, complaints, individual rights requests	164.530(a)			
Patient Complaints <ul style="list-style-type: none"> <li>P&amp;P for patients to make complaints on handling of PHI</li> <li>Form for reporting complaints</li> <li>Process for tracking resolution</li> </ul>	164.530(a), (d), (g)			
Retaliation/Waiver of Rights <ul style="list-style-type: none"> <li>Assure no retaliation and no waiver of rights required</li> </ul>	164.530(g); 164.530(h)			
Sanctions Policy <ul style="list-style-type: none"> <li>P&amp;P for handling HIPAA or other privacy violations</li> <li>P&amp;P for documenting sanctions</li> </ul>	164.530(e)			
Mitigation <ul style="list-style-type: none"> <li>Policy to mitigate harmful effects of improper Uses/Disclosures</li> </ul>	164.530(f)			
Documentation and Record Retention <ul style="list-style-type: none"> <li>P&amp;Ps for compliance and retention</li> <li>Record destruction policy</li> <li>P&amp;Ps for disposal of paper PHI and electronic media PHI</li> <li>Reconstruction of lost medical record</li> <li>Offsite storage</li> <li>Statement of destruction</li> </ul>	164.530(j); 164.504(e)(2) 164.504(f)(2) H142.308(b)(2)	State & Federal record retention laws		

# HIPAA Compliance Task List

<b>TASK DESCRIPTIONS BY TYPE</b>	<b>HIPAA Reg.</b>	<b>Other Legis.</b>	<b>Assigned to</b>	<b>Status</b>
<b>VI. Group Health Plans</b>				
Potential of P&Ps listed above, PLUS, if employer receives PHI: <ul style="list-style-type: none"> <li>Plan document amendment and certification</li> <li>P&amp;Ps to establish "firewalls"</li> </ul>	164.514(g); 164.504(f); 164.530(k)			
<b>HIPAA SECURITY RULE (DRAFT – SUBJECT TO CHANGE)</b>				
<b>I. General Issues - Administration</b>				
Designation of Security Officer <ul style="list-style-type: none"> <li>Security Officer Job Description</li> <li>RBA, Recommendation, Decision</li> </ul>	142.308(b)			
Security of Paper Records <ul style="list-style-type: none"> <li>P&amp;Ps</li> </ul>	164.530(c)			
Reporting and responding to incidents <ul style="list-style-type: none"> <li>P&amp;Ps for workforce</li> <li>Form for reporting</li> <li>Form letter(s) for responding</li> <li>Resolution tracking process/system</li> </ul>	142.308(a)(9)			
Sanctions <ul style="list-style-type: none"> <li>P&amp;Ps for handling security violations</li> <li>Procedure for documenting sanctions</li> </ul>	142.308(a)(10)			
Personnel Security Policy <ul style="list-style-type: none"> <li>Termination procedures</li> <li>Manager Responsibilities</li> <li>User Responsibilities</li> </ul>	142.308(a)(11); 142.308(a)(7)			
<b>II. Access Controls</b>				
Information Systems Access <ul style="list-style-type: none"> <li>P&amp;Ps for determining access</li> <li>P&amp;Ps for granting/changing access</li> <li>P&amp;Ps for terminating access</li> </ul>	142.308(a)(5); 142.308(c)(1)			
Passwords <ul style="list-style-type: none"> <li>P&amp;Ps for voice mail passwords</li> <li>P&amp;Ps for system/LAN passwords</li> <li>P&amp;Ps for facility access</li> </ul>	142.308(a)(5); 142.308(c)(1)			

# HIPAA Compliance Task List

<b>TASK DESCRIPTIONS BY TYPE</b>	<b>HIPAA Reg.</b>	<b>Other Legis.</b>	<b>Assigned to</b>	<b>Status</b>
Remote Access <ul style="list-style-type: none"> <li>• P&amp;Ps for remote access to systems by workforce</li> <li>• P&amp;Ps for remote access to systems by business associates</li> <li>• P&amp;Ps for remote access to systems by other external users</li> </ul>	142.308(d); 142.308(a)(5); 142.308(c)(1)			
<b>III. Security Controls</b>				
Audit Procedures and Controls	142.308(e)(2); 142.308(a)(6)			
Email <ul style="list-style-type: none"> <li>• P&amp;Ps for internal use</li> <li>• P&amp;Ps for external use</li> <li>• P&amp;Ps for retention of what, how and for how long</li> </ul>	142.308(d)			
Portable Equipment <ul style="list-style-type: none"> <li>• P&amp;Ps on use of pagers, laptops, PDAs and cell phones for PHI</li> </ul>	142.308(c); 142.308(d)			
Media Controls Policy <ul style="list-style-type: none"> <li>• Receipt and Removal</li> <li>• Disposal of Equipment</li> </ul>	142.308(b)(2);			
Visitors <ul style="list-style-type: none"> <li>• P&amp;Ps for physical access control</li> </ul>	142.308(b)			
Workforce <ul style="list-style-type: none"> <li>• P&amp;Ps for physical access control</li> </ul>	142.308(b)			
Network Security <ul style="list-style-type: none"> <li>• P&amp;Ps regarding access</li> <li>• P&amp;Ps regarding tampering and unauthorized entry or access</li> <li>• P&amp;Ps to protect and encrypt transmitted PHI per HIPAA regs.</li> <li>• Virus protection</li> </ul>	142.308(c-d) 142.308(a)(8)			
Configuration Management <ul style="list-style-type: none"> <li>• P&amp;Ps for installation of hard/software</li> <li>• P&amp;Ps for removal of hard/software</li> </ul>	142.308(a)(8)			

## HIPAA Compliance Task List

TASK DESCRIPTIONS BY TYPE	HIPAA Reg.	Other Legis.	Assigned to	Status
Workstations <ul style="list-style-type: none"> <li>• P&amp;Ps regarding automatic logoff, screensaver passwords</li> <li>• P&amp;Ps regarding monitor placement</li> <li>• P&amp;Ps regarding printer/fax placement</li> </ul>	142.308(b)			
Chain of Trust Agreements <ul style="list-style-type: none"> <li>• P&amp;Ps to establish definition and need</li> <li>• P&amp;Ps to establish maintenance and renewal of the agreements</li> <li>• P&amp;Ps on combining with other contracts and/or agreements</li> </ul>	142.308(a)(2); 164.502(e) 164.504(e)			