HOLLAND&HART LLP

HIPAA PRIVACY CHECKLIST

The following summarizes required and recommended privacy policies and forms per the HIPAA Privacy Rule. Additional policies are required by the HIPAA Security Rule. Covered entities and business associates should ensure that they have required policies in place to minimize or avoid penalties under the HIPAA regulations. The citations are to 45 CFR Part 164. For additional resources concerning Privacy Rule requirements and compliance assistance, see the Office of Civil Rights privacy website, http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html. The Privacy Rule is subject to periodic amendment. Users should review the current rule requirements to ensure continued compliance.

Policies		
HIPAA Privacy Rule Reference	**Policy**	**Status (Complete, N/A)**
Use and Disclosure: General Rules		
164.506	Consent is implied for treatment, payment and health care operations; no written authorization is required except for psychotherapy notes.	
164.510	Providing notice and chance for patient to agree or object is sufficient for certain disclosures, including disclosures to family members or others involved in the patient's care; for facility directories; and to provide notice in emergency situations.	
164.512	Certain disclosures may be made per regulatory exceptions subject to specific conditions, e.g., uses or disclosures required by law; to avert a serious and imminent health; for public health activities; in response to a court order or subpoena; to law enforcement, etc.	
164.508	Authorizations are generally required for all other uses or disclosures, including uses or disclosures of psychotherapy notes; for most marketing activities; sale of protected health information; etc. Include the elements for a valid authorization.	
Use and Disclosure: Special Rules		
164.514(f)	Fund raising uses or disclosures generally require authorization except in limited circumstances.	
164.512(i)	Research generally requires authorization unless certain conditions are met.	
164.502(f)	Privacy protection continues after death for a period of 50 years.	
164.502(g)	Personal representatives and parents of unemancipated minors are generally entitled to access information and exercise other patient rights, subject to certain exceptions.	
164.514(h)	Covered entities should verify a requesting person's identity and authority before disclosing information.	

Kim C. Stanger
Phone (208) 383-3913
kcstanger@hollandhart.com
www.hollandhart.com

HIPAA Privacy Rule Reference	Policy	Status (Complete, N/A)
164.502(d); 164.514(e)	Covered entities may "de-identify" information, thereby avoiding HIPAA restrictions.	
164.530(c)	Safeguards for facsimiles, e-mails, and telephone communications may be appropriate. (Not expressly required by privacy regulations, but may help satisfy safeguards per 164.530(c))	
Minimum Necessary Standard		
164.502(b)	Limit use or disclosure to the minimum necessary to accomplish the purpose, subject to specified situations.	
164.514(d)	Define and limit workforce members' access to protected information.	
164.514(d)	Establish protocols for routine disclosures, and processes for handling others on an individual basis.	
164.514(d)	Establish protocols for routine requests for information, and processes for handling others on an individual basis.	
164.514(d)	Do not request entire record if not necessary.	
Patient Rights		
164.522(a)	Right to request additional restrictions on use or disclosure for treatment, payment or health care operations; however, the provider is not obligated to agree to restrictions except in limited situation.	
164.522(b)	Right to request alternative means or location of communications, including process for requesting alternatives and limitations on requests.	
164.524	Right to access protected health information, including process for requesting access; time limits and process for responding; bases for denials; and determination of reasonable costs.	
164.526	Right to amend protected health info, including process for requesting amendments; time limits and process for responding; bases and process for denials; attaching amendments or requests; and notifying others about requests.	
164.528	Right to request accounting of protected health information, including process for capturing information for accounting; process for requesting accounting; time limits and process for responding; and limitations on requests.	
Notice of Privacy Practices		
164.520	Provision and posting of notice.	
164.520	Good faith efforts to obtain acknowledgment.	
Business Associates		
164.502(e); 164.504(e)	Process for obtaining business associate contracts; taking action for violations; and obtaining information from business associates to comply with provider's responsibilities.	

Kim C. Stanger
Phone (208) 383-3913
kcstanger@hollandhart.com
www.hollandhart.com

HIPAA Privacy Rule Reference	Policy	Status (Complete, N/A)
Notification Requirements for Breaches of Unsecured Protected Health Information		
164.402	Identifying when a breach occurs.	
164.402	Securing protected health information.	
164.404	Notice to individuals, including timing, content, and providing substitute notice.	
164.408	Notice to HHS, including annual and immediate notices to HHS, timing, and content. The HHS electronic reporting process may be accessed through the OCR's HIPAA website, http://www.hhs.gov/ocr/privacy/.	
164.406	Notice to the media, including form, timing and content.	
164.410	Notice by business associates, including timing and required information.	
164.412	Delay in notice at request of law enforcement.	
Administrative Requirements		
164.530(a)	Designation of privacy offer and contact person.	
164.530(b)	Training existing and new members of the workforce.	
164.530(c)	Use of technical, administrative, and physical safeguards to avoid improper or incidental disclosures.	
164.530(e)	Sanctions against workforce members for violation of policies and regulations.	
164.530(d)	Patient complaints, including the process for complaining and responding to complaints.	
164.530(f)	Mitigation of improper disclosures.	
160.410	Correction of any violations within 30 days to avoid penalties.	
164.530(g)	No retaliation or intimidation against patients or others who exercise HIPAA rights.	
164.530(h)	No conditioning treatment on a waiver of HIPAA rights.	
164.530(i)	Document retention, including identifying documents that must be retained and period of retention.	
Forms		
HIPAA Privacy Rule Reference	**Form**	**Status (Complete, N/A)**
164.520	Notice of privacy practices.	
164.520	Acknowledgment of receipt of privacy practices.	
164.504(e)	Business associate contract.	
164.514(e)	Data use agreement (if used).	
Use and Disclosure Forms		
164.508(c)	Authorization	
164.510	Objection to disclosure per 164.510.	
164.514(f)	Opt-out of fundraising.	
Patient Rights Forms		

Kim C. Stanger
Phone (208) 383-3913
kcstanger@hollandhart.com
www.hollandhart.com

HIPAA Privacy Rule Reference	Policy	Status (Complete, N/A)
164.522(a)	Request for additional restrictions on use or disclosure / denial of request. • Notice of denial of request.	
164.522(b)	Request for alternative means or location for communication / action on request. • Notice of denial of request.	
164.524; 164.524(d)	Request for access to information / action on request. • Notice of denial of request.	
164.526 164.526(d)	Request for amendment of information / action on request. • Notice of denial of request.	
164.528 164.528(b) 164.528	Request for accounting of information / action on request. • Accounting log. • Notice of denial of request.	
Administrative Requirements		
164.530(a)	Privacy officer designation.	
164.530(a)	Contact officer designation.	
164.530(b)	Employee training certification.	
164.530(d)	Complaint form / action on complaint.	
164.530(f)	Privacy violation report form / action in response to incident (including documentation of sanctions).	
164.408	Log of breaches reportable to HHS on annual basis.	

Kim C. Stanger
Phone (208) 383-3913
kcstanger@hollandhart.com
www.hollandhart.com