

HIPAA Checklist

The Field Force Manager application is designed to aid home health aides and nurses in the delivery of care at patient locations. The company providing the service is considered a non-covered entity by HIPAA guidelines. The application is considered a Business Associate (BA) and for a covered entity to be compliant with HIPAA the solution delivered by the BA must follow the Safeguards Principle:

For more information on Privacy Rule and Safeguards Principle

<http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/safeguards.pdf>

Policy	Yes	No	Do Not Need
HIPAA Compliance:			
(1) Privacy Officer – Sr. Director of IT and Wireless Security	X		
(2) Risk analysis – Annual security / privacy audit	X		
(3) Employee Training – All employees undergo annual security/privacy training	X		
(4) Discipline / Sanction Policy – All employees sign secrecy agreement	X		
(5) Personnel Termination Security – All employees sign secrecy agreement	X		
General Confidentiality:			
(6) Health information security - All data is secured	X		
(7) Medical records security – All data is secured	X		
(8) Identification of Protected Health Information – All data and access is tracked	X		
(9) Records confidentiality (42 CFR Part 2)			X
(10) Mental Health Confidentiality			X
(11) Psychotherapy Notes			X
(12) HIV Confidentiality			X
(13) Minimum necessary standard requirements			X
Policies on Disclosure:			
(14) Uses and disclosures of de-identified protected health Information			X
(15) Disclosures to Business Associates – In breach customers would be notified	X		
(16) Disclosures to Qualified Service Organizations			X
(17) Disclosures to Client			X
(18) Disclosures to Minor Clients (emancipated and un-emancipated)			X
(19) Disclosures to Parents of Minor Clients			X
(20) Disclosures to Deceased Individuals			X
(21) Disclosures to Personal Representatives			X
(22) Disclosures for Incompetent Persons			X

(23) Disclosures for Medical Emergencies			X
(24) Disclosures in “Duty to Warn” cases			X
(25) Disclosures for Audit and Evaluations			X
(26) Disclosures for Research			X
(27) Disclosures for Child Abuse/Neglect			X
(28) Disclosures for Elder Abuse			X
Policies on Disclosure: (cont.)			
(29) Disclosures for Domestic Violence			X
(30) Disclosures to Public Health Authorities			X
(31) Disclosures to Law Enforcement from crime on program premises or against program personnel			X
(32) Disclosures for other Law Enforcement purposes			X
(33) Disclosures under Search Warrants			X
(34) Disclosures under Arrest Warrants			X
(35) Disclosures pursuant to Court Orders			X
(36) Disclosures about past crimes			X
Policy	Yes	No	Do Not Need
(37) Disclosures to criminal justice agencies with Consent			X
(38) Disclosures to Government			X
(39) Disclosures for Worker’s Compensation			X
(40) Disclosures for judicial and administrative proceedings			X
(41) Disclosures for Health Oversight / QI Activities			X
(42) Disclosures for Facility Directories			X
(43) Disclosures for involvement in the individual’s care			X
(44) Disclosures to affiliated entities			X
(45) Disclosures for the purpose of treatment			X
(46) Disclosures for the purpose of payment			X
(47) Disclosures for marketing			X
(48) Disclosures to Persons exposed to Communicable Diseases			X
(49) Disclosures for Criminal Health Care Fraud Investigations			X
(50) Disclosures for government health data system			X
(51) Disclosures to patient’s next of kin / friend			X
(52) Disclosures to armed forces			X
(53) Disclosure by Whistleblowers			X
(54) Disclosure to Other Program Staff			X
Patient’s Rights:			
(55) Patients’ rights under HIPAA			X
(56) Patient Education			X
(57) Inspection and Copying of Patients Records			X
(58) Patient Accounting of Disclosures			X
(59) Patient Complaints			X
(60) Patients with Communication Barriers			X
Consent:			
(61) Consent requirements			X

(62) Revocation of Consent			X
MIS Issues:			
(63) Ongoing compliance security audits – Annual security audit	X		
(64) Security testing – Annual security audit	X		
(65) Control access (passwords, etc.) – See security overview	X		
(66) Virus checking – See security overview	X		
(67) Data integrity – See security overview	X		
(68) Data back-up plans – See security overview	X		
(69) Disaster recovery and disaster plan – See security overview	X		
(70) E-mail policy – See employee security agreement	X		
(71) Internet/web-site use and access – See employee security agreement	X		
(72) Portable computer/laptop computer use – See employee security agreement	X		
(73) Facsimile use			X
(74) Encryption – See security overview	X		
(75) Software use – See security overview	X		
(76) Equipment security – See employee security agreement	X		
(77) Internal Reporting for Breach of Security / Confidentiality – see security overview	X		
Policy	Yes	No	Do Not Need
(78) Electronic Signature (including OASA regulations, 77 ILCS 2060.325)			X
(79) Workstation use – see employee security agreement	X		
Billing Policies:			
(80) Medicare / Medicaid Billing			X
(81) Health Insurance Billing			X
(82) Third Party Payer Billing			X
(83) State and federal law compliance			X
(84) State agency recoupment			X
General Record Retention:			
(85) Revision procedures			X
(86) Physical safeguards – see security overview	X		
(87) Contingency plan – see security overview	X		
(88) Record retention – see security overview	X		
(89) Destruction of records policy – see security overview	X		