Privacy and Security Policies of BSHC

The following policy and procedure handbook is developed to assure compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH)[1]. Under this law, BSHC is considered to be a "Covered Entity," subject to all the privacy and security regulations of the act. No staff member can either internally use or externally disclose any consumer's individually identifiable health information (called PHI, protected health information) except as permitted or required by HIPAA.

HIPAA does not overrule Massachusetts' confidentiality laws where state law is more stringent, i.e., more protective of an individual's PHI or rights regarding PHI. [2] This handbook incorporates all state requirements that are more stringent than HIPAA.

The *Standards for Privacy of Individually Identifiable Health Information* ("Privacy Rule") established, for the first time, a set of national standards for the protection of certain health information. A major goal of the Privacy Rule is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well-being. The Rule strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing. Given that the health care marketplace is diverse, the Rule is designed to be flexible and comprehensive to cover the variety of uses and disclosures that need to be addressed.[3]

[1] Federal Register Vol. 78, No.17, January 25, 2013

[2] Applicable state rules regarding privacy and confidentiality are found in MGL c. 66a, MGL c. 93H, Executive Order 504, 651 CMR 5.20, 801 CMR 3.00, 201 CMR 17.00, and EOEA PI 97-55.

[3] http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/

Table of Contents

Definitions

Aging Service Access Point (ASAP) – A state designation for private non-profit agencies like BSHC that are under contract with the Executive Office of Elder Affairs to implement the coordination and delivery of Community-Based Long Term care services. Includes information and referral, case management, coordinating and authorizing the delivery of home care services, clinical screening for nursing facilities, protective services, and in nutrition services.

Business Associate - a person or entity who, on behalf of BSHC, creates, receives, maintains, or transmits protected health information for a function or activity

Executive Office of Elder Affairs (EOEA) – The state unit on aging in Massachusetts mandated to implement and administer services designed to insure the dignity and independence of elders. Also called the Department of Elder Affairs. Is a cabinet level agency under the Executive Office of Health and Human Services.

Health Care Provider – Entity that provides care, services, or supplies related to the health of an individual. This includes, but is not limited to preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual… and sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription. Health Care providers do not require a Business Associates Agreement (BAA)

Protected Health Information (PHI) - any information, whether oral or recorded in any form or medium that relates to the past, present or future physical or mental health condition of a consumer; the provision of health care to a consumer; or the past, present or future payment for the provision of health care to a consumer and can be used to identify the person. Individually identifiable health information includes many common identifiers (e.g. name, address, birth date, SSN)

Privacy Official – Individual at BSHC serving as first point of contact regarding HIPAA related issues. Verifies the identity or authority of any person requesting confidential consumer healthcare information if the identity or the authority of the person is unknown and answers internal HIPAA related questions for agency staff.

Subcontractor - a person [or organization] to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of the business associate

Vendor Agency – An independent organization which contracts with BSHC for the provision of a service(s) specified within a contract.

I. General Organizational Policies

1. Covered Entities

A covered entity is defined as any "health plan, health care clearinghouse, or health care provider who transmits any health information in electronic form in connection with a transaction covered by the HIPAA Privacy Rule."[4]

Health care is defined in the HIPAA regulations in part as, "preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body…"[5]

BSHC is a covered entity because we exchange protected health information (PHI) and therefore must comply with all of the standards and requirements of the Privacy Rule.

1. Business Associates

A business associate is defined as a person or entity who, "on behalf of a covered entity (BSHC)…creates, receives, maintains, or transmits protected health information for a function or activity…including...data analysis, utilization review, quality assurance... [and/or]…provides legal, actuarial, accounting, consulting…for the covered entity…where the provision of the service involves the disclosure of protected health information…from such covered entity…or from another business associate of such covered entity… "[6] Members of BSHC's staff are not business associates.

Please note that a business associate is defined by its function, not through the establishment of a contract with BSHC. Thus, even in the absence of a Business Associates Agreement, the business associate is civilly and criminally responsible for violations of the Privacy Rule. For compliance, a business associate is directly liable or the following:

- Impermissible uses and disclosures;
- Failure to provide access to a copy of electronic protected health information to either BSHC or the individual, or the individual's designee;
- Failure to disclose protected health information where required by the Secretary to investigate or determine the business associate's compliance with HIPAA rules;
- Failure to provide an accounting of disclosures;
- Failure to comply with the requirements of the Security Rule.

A business associate does not include "a health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual." [7] Thus, a Business Associates Agreement is not required with certain BSHC vendors or other health care providers, as long as the reason for the disclosure is limited to providing or coordinating health care. BSHC maintains Business Associate Agreements with agencies whose services fall outside the definition of "health care". Health care is defined as "care,

[4] 45 CFR § 160.103
[5] 45 CFR § 160.103
[6] 45 CFR § 160.103
[7] 45 CFR § 160.103

services, or supplies related to the health of an individual. Health care includes, but is not limited to, the following: 1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual… and 2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription" (emphasis added).[8] In other words, the definition is very broad, and includes many of the services BSHC provides to consumers; for example, personal care, adult day health, and habilitation therapy.

When BSHC enters into a new agreement, the Quality Assurance Department determines whether a BAA is required. If a BSHC contractor provides a service defined as health care as well as other services not so defined, a BAA is not required. The requirement stands only for providers for which the definition of 'health care provider' cannot apply. For example, Agency A provides personal care ("health care" as defined in the statute) and chore (not "health care" as defined in the statute). In this case, no BAA is required. On the other hand, Agency B provides chore only, or chore and laundry (not "health care" in either case). In this case, a BAA is required. In the appendices are lists of EOEA approved services for which BSHC maintains BAAs.

A covered entity can be the business associate of another covered entity when the function or activity performed on its behalf is that of a business associate. For example, when BSHC conducts joint vendor monitoring, another ASAP may act as the business associate of the other, and a Business Associates Agreement is required.

In addition to covered entities and business associates, the revised rule defines another category of entity, subcontractors. A subcontractor is defined as, "a person [or organization] to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of the business associate."[9] A Business Associate is permitted to release PHI to a subcontractor if it has a contract (Business Associates Agreement) with the subcontractor that meets the requirements of HIPAA and extends certain provisions of HIPAA to the subcontractor.[10] As entities that create, receive, maintain, or transmit PHI on behalf of a business associate, a subcontractor is also therefore a business associate.[11]BSHC is not required to hold BAAs with subcontractors of its business associates.

In addition to subcontracted service providers, there are other entities, such as auditors, law firms, housing advocates, etc., to whom BSHC discloses consumer information, and with whom a BAA is held.

Examples:

- A researcher is not a business associate, as research is not an activity regulated by the HIPAA rules;
- An Internet Service Provider (ISP) is not a business associate, as it falls within the "conduit exception;"
- An independent auditor is a business associate, as accounting is one of the services listed in the definition of business associate;
- A data destruction company is a business associate; as it receives PHI and performs an activity within the definition of "health care operations;"
- A janitorial service is not a business associate, as its access to PHI would be purely incidental;
- A bank that is solely engaged in processing payments for health care is not a business associate, as § 1179 of the HIPAA statute exempts certain activities of financial institutions from the HIPAA rules, although a bank that engaged in other activities regulated by HIPAA could be a business associate.

[8] CFR 45 § 160.103
[9] 45 CFR § 160.103
[10] 45 CFR § 164.502(e)(1)
[11] 45 CFR § 160.103 (ii)

Under HIPAA, compliance reviews are the responsibility of the Secretary of Health and Human Services.[12] BSHC is not required to monitor the HIPAA compliance of other entities covered by the HIPAA privacy regulations. In the case of business associates, BSHC has the responsibility to attempt to correct any violations of the BAA.[13] Specifically, BSHC must "[take] reasonable steps to cure the breach or end the violation…and, if such steps were unsuccessful, [terminate] the contract, if feasible, or [report] the problem to the Secretary [of Health and Human Services]."[14]

Records of all BAA's must be retained "for six years from the date of its creation or the date when it last was in effect, whichever is later."[15]

Summary:

- BSHC is a covered entity under HIPAA and must comply with all of the rules
- BSHC does not monitor HIPAA compliance for contracted vendors who are covered entities under HIPAA
- BSHC maintains Business Associate Agreements with agencies whose services fall outside the definition of "health care"
- BSHC is responsible for correcting the HIPAA violations of its business associates

II. Release of Information

It is the policy of BSHC that individuals have the right to have their individual health care information be treated as confidential and private.

Information regarding deceased consumers of BSHC shall be afforded all the protections granted under the Privacy Rule and Elder Affairs regulations.[16] BSHC must treat the executor, administrator, or other person authorized to act on behalf of a deceased individual as a personal representative of the deceased consumer.[17]

1. What is Health Information?

The HIPAA Privacy Rule define health information as, …"any information, whether oral or recorded in any form or medium, that is created or received by BSHC and relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past present or future payment for the provision of health care to an individual."[18] This includes all information BSHC holds about a consumer: name, address, phone number, status as a consumer of BSHC, the services the consumer receives through BSHC, as well as medical/social diagnosis, FIL category, etc. All of this information is considered to be protected health information (PHI), and may not be used or disclosed, except as provided for by the Privacy Rule or state law, where the state law is more stringent.

[12] CFR 45 § 160.308
[13] See CFR 45 § 164.504 (e)(1)(2)
[14] CFR 45 § 164.504 (e)(ii)
[15] CFR 45 164.530 (j)
[16] The revised Rule states that the requirements of HIPAA must be complied with for 50 years following the death of an individual. See 45 CFR § 164.502(f). As Massachusetts laws and regulations do not have a similar sunset provision, and as covered entities are required by HIPAA to follow state law in cases where state law is more stringent, the new rule is not incorporated here.
[17] 45 CFR § 164.502(g)(4)
[18] 45 CFR § 160.103

2. Permitted Uses and Disclosures

A. Use and Disclosure

The Privacy Rule contains many provisions that describe the permitted and/or required uses and disclosures of protected health information. This policy and others relating to the release of consumer information incorporate the confidentiality policy previously established by the Executive Office of Elder Affairs[19] and those provisions of HIPAA most relevant to the operations of BSHC. Requests for the use or disclosure of consumer information not addressed in these policies nevertheless may arise. All such requests must be immediately referred to the HIPAA Privacy Official of BSHC, the Director of Development & Quality Assurance. It is the responsibility of the Privacy Official to ensure that responses to such requests are compliant with all applicable Massachusetts law, Elder Affairs regulations, and federal regulations.

The Privacy Rule permits the following uses and disclosures of PHI:[20]

1. To the consumer who is the subject of the data
2. For treatment, payment, or health care operations
3. Incident to a use or disclosure that is permitted by the Privacy Rule, provided that BSHC has met the 'minimum necessary' standards and has instituted safeguards to prevent unauthorized disclosures of PHI
4. Pursuant to a valid authorization that complies with the applicable sections of the Privacy Rule
5. A limited amount of personal data may be released in specific circumstances with the consumer's verbal agreement

The Privacy Rule prohibits the following uses and disclosures of PHI:[21]

1. Use and disclosure of genetic information for underwriting purposes;
2. Sale of protected health information.

The Privacy Rule also details a number of circumstances, such as health oversight and law enforcement activities, in which PHI may be released without authorization or agreement from the consumer.[22] All such requests must be referred to the Privacy Official, except as otherwise noted. It is the responsibility of the Privacy Official to verify the identity or authority of any person requesting confidential consumer healthcare information if the identity or the authority of the person is unknown.[23] If the request is in writing, the letter shall be written on the appropriate agency or government letterhead.

Personal Representatives

The Privacy Rule affords to a 'personal representative' all the rights and considerations afforded to the individual subject of the PHI.[24] Thus, a covered entity or business associate must share information with a personal representative as though he or she were the Consumer. The Privacy Rule defines a personal representative as a person who, "…under applicable law…has authority to act on behalf of an individual…in making decisions related to health care…"[25]

---

[19] EOEA PI-97-55
[20] 45 CFR § 164.502 (a)(1)
[21] 45 CFR § 164.502(a)(5)
[22] 45 CFR § 164.512
[23] 45 CFR § 164.514(h)(1)
[24] 45 CFR § 164.502(g)(1)
[25] 45 CFR § 164.502(g)(2)

The extent to which a person can act as a personal representative, and thus the right to receive PHI that that person has, is limited by their authority to act on behalf of an individual/consumer under applicable state law. For example, if the action of a Health Care Proxy is limited to making decisions about the provision of life-sustaining medical treatments for the consumer, then the covered entity may only share PHI that relates to that health issue. On the other hand, if the health care proxy is unrestricted, and, importantly, invoked, then the covered entity must treat the personal representative as the consumer. A guardian would have unrestricted access to PHI and is empowered to act fully on the consumer's behalf in other areas regulated by the Privacy Rule, such as authorizations and requests to amend PHI.

B. Treatment, payment, and health care operations

BSHC may use or disclose PHI for its own treatment, payment, or healthcare operations. [26] Any use or disclosure for reasons other than treatment, payment, or health care operations must be approved by the Privacy Official of BSHC, unless otherwise noted.

Treatment

Treatment is defined as, "the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultations between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another."[27] There are no restrictions on sharing information with other health care providers for the purpose of providing treatment to a consumer, except for information regarding a consumer's HIV status.[28] In order to disclose this information for any reason, BSHC must obtain a signed EOEA form, Authorization for Disclosure of HIV Status.

Most of the agencies that provide services directly to the consumer are considered "health care providers" under the definition in the Privacy Rule. Those vendors that are not so considered have signed a Business Associates Agreement that permits BSHC to disclose essential consumer information to them, and that restricts the manner in which they may use such information.

Situations may arise in which the interest of the consumer may be served by a disclosure of PHI, but the individual or agency to whom the disclosure is to be made is neither a health care provider nor a business associate; e.g., a legal services agency. In these cases, a signed authorization may be required. Such instances may be discussed with the Privacy Official, who will attempt to execute a Business Associates Agreement with the individual or agency identified.

Payment

BSHC may disclose PHI for its own payment activities. If disclosures for this purpose are to be made to a relative, friend, or other caregiver, the consumer must be given an opportunity to agree or object prior to the disclosure. (See the policy in this manual on Uses and Disclosures Requiring an Opportunity for the Individual to Agree or Object.) In addition, BSHC may disclose PHI to, "another covered entity or a health care provider for the payment activities of the entity that receives the information."[29]

[26] 45 CFR § 164.506(c)(1)
[27] 45 CFR § 164.501
[28] MGL c. 111 § 70F
[29] 45 CFR § 164.506(c)(3)

Health Care Operations

The definition of health care operations is extensive, and includes quality assessment and improvement activities, performance evaluation, training programs (including those involving students), conducting or arranging for legal services and auditing functions, business planning and development, and resolution of internal grievances.[30] Any agency or individual not employed by BSHC that participates in or is contracted to provide services relating to health care operations that entails the use or disclosure of PHI must sign a Business Associates Agreement.

C. Informed Consent

Pursuant to 801 CMR 3.00, Elder Affairs requires informed consent for the holding and releasing of personal information.[31] However, under HIPAA, informed consent is insufficient to authorize the use or disclosure of PHI for any purpose that would require a valid authorization under its (HIPAA's) terms.

If a BSHC staff member receives a request to release or disclose PHI, for reasons other than treatment, payment, or health care operations, the staff member must inform his/her supervisor and send an email to the Privacy Official immediately for guidance on follow up.

3. Minimum Necessary Standard

The Privacy Rule states that, "When using or disclosing protected health information or when requesting protected health information from another covered entity or business associate, a covered entity or business associate must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request."[32] The use or disclosure of PHI to another health care provider for treatment purposes is *specifically excepted from this rule*.[33] Other exceptions include disclosures to the individual who is the subject of the PHI (the consumer), disclosures made pursuant to a valid authorization, and other disclosures required by law.[34]

The minimum necessary standard as it relates to use concerns the restriction of employee access based on the employee's function. The minimum necessary standard as it relates to disclosure, because it does not apply to treatment, should be applied in the context of payment, health care operations, and certain other disclosures approved by the Privacy Official.

A. Employee Access

Only those employees directly involved in the consumer's care for the purpose of providing service, billing, or a function of health care operations shall have access to the consumer's record. The Privacy Rule requires BSHC to identify classes of employees who require access to PHI, the categories of PHI to which they require access to carry out their duties, and any conditions upon access.[35]

[30] See 45 CFR § 164.501 for the full definition.
[31] 801 CMR 3.02(2)
[32] 45 CFR § 164.502(b)(1)
[33] 45 CFR § 164.502(b)(2)(i)
[34] 45 CFR § 164.502(b)(2)
[35] 45 CFR § 164.514(d)(2)(i)

Information and Referral Staff: Access to consumer key facts, care management information, and progress notes.

Fiscal Staff: Access to information that relates to billing and payment, which may include, but is not limited to, cost share amount, service assignment, income, and progress notes.

Administrative Staff: Access to consumer information required for clerical processing of files, authorizations, mailings, referrals, screenings, and other administrative duties.

Volunteers, Students, or other temporary staff: Strictly limited access depending on function. In each case, the immediate supervisor will be responsible for determining the exact level of access.

The following personnel shall have unrestricted access to PHI: Care Managers, Nurses, Information Systems staff, and Management.

Nevertheless, those categories of persons granted full access are not permitted to access PHI for individuals for reasons other than treatment, payment, or health care operations, or for other reasons permitted or required under the Privacy Rule or state law or regulation.

All staff are regularly reminded and updated regarding HIPAA and Privacy Rule compliance regulations on a quarterly basis via email communication from the Director of Development & Quality Assurance. BSHC also conducts annual HIPPA refresher training for all employees.

B. Payment and Health Care Operations

The Privacy Rule requires BSHC to develop policies that limit the amount of PHI that it discloses on a routine and recurring basis.[36]

If it is necessary to contact a spouse, guardian, or other caregiver of a consumer for the purpose of discussing cost share payments of the consumer, or if such a person contacts BSHC regarding cost share payments, the information disclosed by fiscal or care management staff to such persons shall be limited to account status and history, and general information regarding services and the consumer's condition. More specific information may be released if circumstances warrant, but such judgment shall be made exclusively by interdisciplinary care management or supervisory staff.

For the purpose of verifying provider invoices, fiscal staff shall limit the disclosure of PHI to eligibility status, service assignment, care management information, and other information that relates to the provision of service, such as dates of suspensions in service.

Individuals or agencies responsible for elements of consumer care may contact BSHC to determine whether or not an individual is a consumer, or to coordinate care with BSHC. The switchboard operator shall not confirm an individual's status as a consumer of BSHC. In order not to impede the coordination of care to an individual, the operator shall check SAMS, and, if the individual is a consumer, transfer the caller to the appropriate care manager. This shall be done without an explicit confirmation of the individual's status as a consumer of BSHC.

For all other disclosures that relate to payment or health care operations, the purpose of the disclosure must be ascertained. The information released must be limited to the amount reasonably necessary to accomplish the purpose of the disclosure. Each such disclosure must be reviewed on an individual basis. Any member of

[36] 45 CFR § 164.514(d)(3)(i)

management staff, including the Privacy Official, may rely on his/her professional judgment to determine the amount and/or type of PHI disclosed.

4. Authorizations for Release of Consumer Information

If a release of PHI is not for reasons relating to treatment, payment, health care operations, or other purposes required or permitted,[37] BSHC must obtain a signed authorization from the consumer for that specific purpose.[38] It is the responsibility of the Privacy Official to ensure that all authorizations meet the standards of the Privacy Rule and Elder Affairs regulations.

An authorization is specifically required by the Privacy Rule for the following:[39]

- Psychotherapy notes (except for certain uses for treatment, payment, or health care operations;
- Marketing, except for face-to-face communications with an individual or promotional gifts of nominal value provided by BSHC;
- Sale of PHI

Authorizations may not be combined with other documents, and the provision of care may not be conditioned upon receipt of an authorization. [40]

Research

PHI shall not be released for research purposes without a valid authorization from the individual. Research sponsored by BSHC must conform to existing policy established by the Executive Office of Elder Affairs.[41] Research not sponsored by BSHC must be approved by the Elder Rights Review Committee.

Procedure for Obtaining Authorizations

In obtaining an authorization from the consumer, BSHC staff must adhere to the following procedure:

1. Staff will review the purpose of the **Release of Information Authorization** with the consumer.
2. Ask the consumer to read, complete, sign and date the authorization form on the designated areas.
3. Explain to the consumer that the authorization form can be revoked at any time. This revocation must be in writing.
4. Send a copy of the form to the consumer, and place the original completed authorization form in the consumer's record.
5. The organization will retain the signed authorization form for a period of seven (7) years from the date the consumer closes.

See the revised authorization form in the appendices.

[37] See the policy on Uses and Disclosures for which an opportunity to agree or object is not required.
[38] 45 CFR § 164.508(a)(1) and EOEA PI-03-17
[39] 45 CFR § 164.508(a)(1)
[40] 45 CFR § 164.508 (b)(3-4)
[41] EOEA PI-03-17

5. Uses and Disclosures Requiring an Opportunity for the Individual to Agree or Object

BSHC may disclose PHI to a family member, relative, or other caregiver when the information is relevant to that person's involvement in the consumer's care or payment related to the consumer's care. BSHC may also disclose PHI to notify, or assist in the notification of, a family member, relative, or other caregiver of the consumer's location, general condition, or death. Prior to such disclosures, the consumer must be given an opportunity to agree or object.[42] BSHC's information and the consumer's agreement may be given orally.[43] HIPAA does not require documentation of an oral agreement or objection.[44]

If the consumer is present, BSHC staff may disclose the information if the consumer agrees, or if the consumer is given an opportunity to object and does not express an objection, or if the staff member, on the basis of his/her professional judgment, reasonably infers from the circumstances that the consumer does not object.[45]

If the consumer is not present or the opportunity to agree or object cannot be practicably provided due to the consumer's incapacity or emergency circumstance, BSHC may disclose PHI directly relevant to the person's involvement in the consumer's care when the disclosure is in the interest of the consumer. In such cases, BSHC is permitted make reasonable inferences based on experience and its professional judgment.[46] Disclosures authorized by this section of the Privacy Rule may also be made after the death of the individual to those persons involved in the individual's care or payment of care, unless doing so violates an expressed preference of the individual of which BSHC is aware.[47]

6. Uses and Disclosures for which an Authorization or an Opportunity to Agree or Object Is Not Required

A. General Rules

The Privacy Rule accounts for many situations in which a covered entity such as BSHC may need to use or disclose PHI without a written authorization or the individual's oral agreement.[48] Any such use or disclosure should only be made by BSHC with the approval of the Privacy Official, the Program Director, or his/her designees, unless otherwise noted. Each use or disclosure described in this policy must be recorded in the progress notes of the consumer record, in accordance with the policy on the Consumer's Right to an Accounting of Disclosures.

The Privacy Rule permits the following uses and disclosures in this section:[49]

- For public health activities, such as medical surveillance of the workplace and workers compensation
- Disclosures about victims of abuse or neglect
- For health oversight activities authorized by law
- For judicial or administrative proceedings

[42] 45 CFR § 164.510(b)(1)
[43] 45 CFR § 164.510
[44] 45 CFR § 164.530(j)(1)(ii) states that communications required to be in writing must be kept as documentation. This excludes oral agreements and oral objections.
[45] 45 CFR § 164.510(b)(2)
[46] 45 CFR § 164.510(b)(3)
[47] 45 CFR § 164.510 (b)(5)
[48] 45 CFR § 164.512
[49] 45 CFR § 164.512

- For law enforcement purposes
- Disclosures regarding decedents to medical examiners or funeral directors, under certain circumstances
- For cadaveric eye, organ, or tissue donation
- For research, within guidelines contained in the Privacy Rule
- To avert a serious threat to health or safety
- For specialized government functions, such as national security and intelligence activities
- For purposes of identification or other activities related to disaster relief

The Privacy Rule permits the release of PHI in response to a subpoena if certain conditions are met.[50] However, state regulation is more stringent on this point and must therefore be followed in preference to HIPAA. EOEA PI-97-55 requires the BSHC to notify the data subject of the subpoena in time to permit the data subject to quash the subpoena. [51]

In addition, covered entities or health plans that are government programs providing public benefits may share information as required by statute or regulation, or for the purpose of coordinating functions or improving administration and management.[52]

B. Fundraising Exception

BSHC may use or release to a business associate or an organization-related foundation limited confidential healthcare information for the purpose of raising funds. [53]

The following confidential health care information may be used or released:

- Consumer demographic information
- Dates of service provided to the consumer
- Department of service information
- Outcome information
- Health insurance status[54]

Demographic information is defined as, "name, address, other contact information, age, gender, and date of birth."[55]

In order to use PHI for fundraising, BSHC includes in its Notice of Privacy Practices a statement that informs consumers of its intent to do so and of the consumer's right to opt out of receiving further fundraising communications.[56]

The organization may not release any other confidential healthcare information for fundraising purposes. In addition, BSHC includes in any fundraising materials sent to a consumer directions on how the consumer can choose to stop receiving any future fundraising materials, and makes reasonable efforts to ensure that those consumers who do not want to receive fundraising materials will be removed from the fundraising mailing list. As required by the Privacy Rule, BSHC's "opt-out" method does not place an undue burden on the consumer.

[50] 45 CFR § 164.512 (e)(1)(ii)
[51] EOEA PI-97-55 § 7(E)
[52] 45 CFR § 164.512(k)(6)(ii)
[53] 45 CFR § 164.514(f)
[54] 45 CFR § 164.514(f)(1)(i-vi)
[55] 45 CFR § 164.514(f)(1)(i)
[56] 45 CFR § 164.514(f)(2)(i)

C. Elder Abuse Reporting

The release of PHI without an authorization from the consumer is permitted under the Privacy Rule for the purpose of reporting abuse, neglect, or domestic violence.[57] The disclosure must be made to the appropriate government authority, such as Protective Services. The disclosure may be made without the consumer's agreement if the BSHC staff person, using his/her professional judgment, "believes the disclosure is necessary to prevent serious harm to the [consumer] or other potential victims…"[58] The Privacy Rule requires BSHC to inform the consumer of the disclosure, except when so informing the consumer would place him/her at risk of serious harm, or when the disclosure would be made to a personal representative BSHC believes to be responsible for the harm to the consumer.[59]

Disclosures to Protective Services must be recorded in the progress notes of the consumer record in accordance with the policy on Right to an Accounting of Disclosures contained in this manual.

7. Required Disclosures[60]

With some exceptions, BSHC must release information to the individual/consumer and/or his/her personal representative. If BSHC has reasonable cause to believe that the individual has been subjected to abuse, violence, or neglect by the personal representative, or, in the professional judgment of BSHC staff, that the releasing of information to that person would not be in the best interest of the consumer or might endanger the consumer, BSHC is not required to release the information. In such cases, the Privacy Official will consult with BSHC's attorney for consumer related issues.

BSHC must release information to the Secretary of Health and Human Services for the purpose of monitoring BSHC' compliance with HIPAA.

[57] 45 CFR § 512.164(c)
[58] 45 CFR § 512.164(c)(1)(iii)(A)
[59] 45 CFR § 512.164(c)(2)
[60] 45 CFR § 164.502(a)(2)

III. Consumer Rights

1. Notice of Privacy Practices

All consumers, including those residing in a Nursing Facility for whom BSHC conducts an on-site clinical assessment, receive written notice of BSHC' privacy practices. Individuals with whom BSHC has a direct treatment relationship (i.e., home care consumers) shall receive the Privacy Notice at the first home visit.[61] For all others, the Privacy Notice will be available upon request.[62]

At the time of the initial home visit and assessment, the Care Manager will provide the consumer with a copy of the Privacy Notice and ask the consumer to sign two copies of the Privacy Notice Acknowledgment Form.[63] The consumer will keep one copy; the other copy will be placed in the consumer's case record. The Privacy Notice Acknowledgment Form will be retained (along with the entire consumer record) for seven (7) years subsequent to the consumer's close date.

Whenever the Notice is revised, BSHC will make the Notice available upon request on or after the effective date of the revision.[64] The NPP is permanently displayed prominently at the entrance to the BSHC office at reception with copies available. The Privacy Notice is posted and can be easily downloaded and viewed on BSHC's website, http://www.bostonseniorhomecare.info/.[65]

A sample notice (NPP) may be found in the appendices.

2. Right to Request Privacy Protection for PHI

The consumer has a right to request that BSHC restrict uses and disclosures of PHI for the purpose of treatment, payment, or health care operations; for a caregiver's involvement in the consumer's care; or for notifying a caregiver of a consumer's location, general condition, or death. [66] All requests must be submitted to BSHC in writing to the BSHC Privacy Official. BSHC is not required to agree to a restriction, except regarding the disclosure of information to a health plan about care or treatment for which the consumer paid in full.[67] (It is not recommended that BSHC agree to a restriction, and, in any case, any such restriction must be approved by the Program Director and the Privacy Official, who shall be jointly responsible for ensuring that BSHC complies with all applicable sections of the Privacy Rule that pertain to agreed-upon restrictions.[68])

A record of any agreement regarding a restriction between BSHC and the consumer, and other documents related to it, must be maintained in the consumer record for a period of seven (7) years from the close date of the consumer record.

BSHC may terminate the restriction agreement only after informing the consumer of the termination of the agreement. Once the consumer is notified, BSHC must maintain the confidentiality of the information in the

[61] 45 CFR § 164.520(c)(2)(i)(A)
[62] 45 CFR § 164.520(c)
[63] 45 CFR § 164.520(c)(2)(i); 45 CFR § 164.520(c)(2)(ii)
[64] 45 CFR § 164.520 (c)(2)(iv)
[65] 45 CFR § 164.520(c)(3)(i)
[66] 45 CFR § 164.522(a)(1)(i)
[67] 45 CFR § 164.522 (a)(1)(ii) and (vi)
[68] See 45 CFR § 164.522 *passim*

original agreement prior to the termination of the agreement. Information accumulated after the notification to terminate the agreement would not be covered or restricted by the terms of the previous agreement.

The organization may terminate an agreement to restrict the use of confidential healthcare information if:

- The consumer agrees or requests the agreement to be terminated in writing.
- The consumer agrees or requests the agreement to be terminated verbally and the termination is documented in the consumer's medical record.
- The organization informs the consumer in writing that the agreement to restrict confidential healthcare information is terminated.

In addition, the consumer has a right to request that communications of PHI (such as cost share bills) be sent by alternative means or at alternative locations.[69] The request must be submitted to BSHC in writing and must include an alternative address or method of contact.[70] It is the responsibility of BSHC to comply with any reasonable request of this kind.[71] BSHC may not condition its compliance upon an explanation from the consumer regarding the basis of the request.[72]

3. Right of Access

The following section describes the various ways a consumer is able to access his/her record. If a BSHC employee receives a request from a consumer or his/her representative to access the consumer record, the employee must notify the Program Director and BSHC Privacy Official for guidance.

Each consumer (data subject) or his/her duly authorized representative has the right to inspect or receive a copy of his/her record, except where prohibited by law or judicial order.[73] Consumer PHI that is compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding is exempted from this standard.[74]

The consumer must make the request to BSHC in writing. Acceptance or denial must be made to the consumer in writing. BSHC may request that the consumer receive a summary of the information contained in the record.

If the request for access is not denied, BSHC must comply with the request within 30 days.[75] BSHC is entitled to one 30-day extension, provided that the consumer is informed of the extension in writing, and such letter includes a date for compliance with the request and an explanation for the extension. [76]

If the consumer elects to inspect the case record, the inspection will take place at the offices of BSHC under the supervision of the Program Director or Privacy Official, or their designees.

[69] 45 CFR § 164.522(b)(1)(i)
[70] 45 CFR § 164.522(b)(2)(i) and 45 CFR § 164.522(b)(2)(ii)
[71] 45 CFR § 164.522(b)(1)(i)
[72] 45 CFR § 164.522(b)(2)(iii)
[73] EOEA PI-97-55; 45 CFR § 164.524(a)(1)
[74] 45 CFR § 164.524(a)(1)(ii)
[75] 45 CFR § 164.524 (b)(2)(i)
[76] 45 CFR § 164.524 (b)(2)(ii)

If the consumer elects to receive a copy of the record, the record must be provided in the form and format, including an electronic format, requested by the consumer, if the record is readily producible in the requested format. If the request for a particular electronic format cannot be accommodated, BSHC may provide the record in a readable electronic format (such as MS Word or Adobe PDF) agreed to by BSHC and the consumer.[77] The consumer may be charged a reasonable amount based on supplies and labor for hard copy records and labor only for electronic records, unless the consumer requests that the record be provided on portable media.[78]

A consumer may request that the copy of the electronic record be provided directly to another individual. Such request must be in writing, signed by the consumer, and clearly identify the designated person and where to send the copy of PHI.

A consumer's request to review his/her case record may be denied under certain circumstances; e.g., when such a disclosure may cause harm to the consumer or another person, or when PHI was obtained from someone other than a health care provider under a promise of confidentiality. Any such circumstances relevant to the disclosure of the contents of the case record to a consumer must be related to the Program Director and Privacy Official who shall be jointly responsible for denying access, and, if access is denied, ensuring that BSHC complies with the rules governing denial of access contained in EOEA PI-97-55 and the Privacy Rule.[79]

In addition, according to Massachusetts law, references to third parties may be deleted from the record, provided that such third persons are not government officials acting as such and the data subject is also not a government official acting as such.[80]

4. Right of Amendment[81]

A. Policy for the Amendment of Consumer Records

The consumer has a right to have BSHC amend PHI about the consumer in the case record for as long as the PHI is maintained. BSHC may deny a consumer's request for amendment if it determines that the PHI:

1. Was not created by BSHC, unless the individual provides a reasonable basis to believe that the originator of the PHI is no longer available to act on a requested amendment
2. Is not part of the case record
3. Would not be available for inspection (see the policy on Consumer Right of Access)
4. Is accurate and complete

A consumer's request to amend PHI must be submitted to BSHC in writing. All such requests must be immediately referred to the Program Director and the Privacy Official, who shall be responsible for responding to the request in accordance with the Privacy Rule.

[77] 45 CFR § 164.524 (c)(2)
[78] 45 CFR § 164.524 (c)(4)
[79] 45 CFR § 164.524 *passim*
[80] MGL 66a § (2)(i)
[81] 45 CFR § 164.526

B. Procedure for the Amendment of Consumer Records

Amendments: Consumer requested changes:

After reviewing healthcare information, the consumer may request that changes be made to information in the record. BSHC will ask the consumer to put the request in writing and include the reasons why the consumer wants changes made to the information**. All such requests shall be referred to the Privacy Official for consultation on how to proceed**. BSHC will have 60 days to act on the request to make changes to the information. If BSHC cannot act on the request within 60 days, the time period can be extended once for an additional 30 days. BSHC must to write the consumer a letter explaining the need and reasons for an additional 30 days and the expected date the decision about the request will be made.

In response to the request to make changes to the healthcare information, BSHC:

- Can deny the request if the information the consumer wants changed was not created by the organization.
- Can deny the request if the individual who created the information that the consumer wants changed is no longer an employee of the organization.
- Can deny the request if the information in the record is currently accurate and complete.

If the corporation denies the request to make changes to the information, the following shall be done:

- Write the consumer a letter explaining the reason(s) for the denial.
- Explain in the denial letter steps the consumer can take to dispute the organization's decision.
- Explain in the denial letter that if the consumer does not dispute the organization's decision, the consumer may request that the organization include the consumer's request for changes and the denial in any future releases of the disputed healthcare information.
- Explain how the consumer can file a formal complaint to the organization with the Privacy Officer.

If BSHC decides to honor the request for changes:

- The organization shall make the changes.
- Inform the consumer that the changes are accepted.
- Obtain from the consumer the names of individuals who need to have the changed information.
- Attempt to reach those individuals who need to have the changed information.
- Attempt to contact other persons or business associates regarding the changed information if the information was detrimental to the consumer.

Document the titles and names of the employees responsible for receiving and processing the request for changes. Documentation will be maintained for a period of seven (7) years after the date the consumer closes.

5. Right to an Accounting of Disclosures[82]

Each consumer has the right to receive an accounting of disclosures of PHI made by BSHC in the six years prior to the date on which the accounting is requested, including disclosures made to or by business associates of BSHC, except for disclosures:

1. To carry out treatment, payment, or health care operations
2. To individuals of PHI about them
3. Incident to a use or disclosure otherwise permitted

[82] 45 CFR § 164.528

4. To persons involved in the individual's care
5. For national security or intelligence purposes
6. To correctional institutions or law enforcement officials
7. That occurred prior to the compliance date for BSHC

The Privacy Official must approve any disclosures of PHI made for any purpose other than for treatment, payment, or health care operations. After receiving approval for specific disclosures, the employee making the disclosure must record the relevant information in a journal entry in the consumer record. (For example, after responding to an inquiry from the Department of Public Health regarding a report of misappropriate of consumer property.) The journal entry must include the date of the disclosure, the name, title, and affiliation of the person who received the PHI, as well as a description of the PHI disclosed and the reason for the disclosure.

The Privacy Official shall compile an accounting of disclosures based on a review of the consumer record. The report to the consumer shall include, for each disclosure:

1. The name of the subject of the PHI
2. The date of the disclosure
3. The name of the entity or person who received the PHI and, if known, the address of such person or entity
4. A brief description of the PHI disclosed
5. A brief statement of the reason for the disclosure, or a copy of a written request

BSHC must act on the individual's request within 60 days. BSHC is entitled to one extension of 30 days, provided BSHC provides the consumer with a written explanation for the delay and a date for compliance. Each consumer may receive one such accounting of disclosures without charge in a 12 month period. A reasonable, cost-based fee may be charged to the consumer for additional reports within the same 12 month period.

IV. Administrative Requirements

1. Personnel Designations[83]

BSHC designates the Director of Quality Improvement as the Privacy Official. The Privacy Official shall be the person who is responsible for receiving complaints regarding the use or disclosure of PHI, and for providing further information about the agency's privacy policies. The Privacy Official is responsible for ensuring the confidentiality of all consumer healthcare information, developing and implementing all policies and procedures affecting consumer confidential healthcare information, limiting the incidental disclosure of protected healthcare information (PHI), and maintaining all documentation required under the Privacy Rule and Elder Affairs regulations.

The Information Technology Manager shall serve as the agency's Security Officer and be responsible for the electronic security of all consumer information. The IT Manager shall evaluate all computer systems and corresponding networks to certify the level of security meets the standards of HIPAA and 201 CMR 17.00.

2. Staff Training

BSHC provides training to all new employees upon hire on privacy policies and procedures, and to all employees on an annual basis. The workforce includes all employees, volunteers, trainees, and other persons whose work is under the direct control of the agency, even if they are unpaid. Such training shall meet the following standards:[84]

1. Train employees as necessary and appropriate to carry out their functions
2. Train staff no later than the compliance date
3. Train new employees within a reasonable amount of time
4. In case of changes, train employees within a reasonable amount of time
5. Document training

3. Safeguards

BSHC has instituted the following safeguards to protect health care information from intentional or unintentional use or disclosure in violation of the Privacy Rule, as well as disclosures incidental to permitted uses and disclosures:[85]

The external doors are locked at all times. Employees use swipe cards to gain access to the office. The receptionist will admit non-authorized personnel only after a staff member has confirmed the purpose of their visit. All visitors are required to wear a visitor's badge at all times, and are escorted by staff when leaving their designated meeting area.

The hard copy of the consumer record shall be maintained in a secure environment and not left unattended in areas accessible by non-authorized individuals. Consumer records must not be kept longer than required by

[83] 45 CFR § 164.530(a)(1); EOEA PI-97-55
[84] 45 CFR § 164.530(b)
[85] 45 CFR § 164.530(c)

regulation or contract.[86] The Privacy Official is responsible for ensuring that consumer records are destroyed after seven years from the date of close, except for records created and maintained pursuant to contracts with Medicare Advantage Plans (SCOs) and Integrated Care Organizations (One Care Plans), which shall be destroyed 10 years after the date of close.

When working with a consumer record, staff must exercise caution to insure that it is not easily read by anyone else. Records should not be left in locations open to the public.

At the end of the day, client files should be locked. Client files must not be left on desks for employees who are not in the office. For CM's and RN's, client files must be placed in their overhead bins and locked

Disposal of client records shall be by shredding. Records that are kept in off-site storage will be destroyed by shredding at the end of seven years from the close date. No identifying information will be thrown in the regular trash.

Except with express Supervisory approval, consumer files are not to be removed from the office. Consumer information carried out of the office must be kept at a minimum, and only for necessary purposes. Intakes, re-determinations, or other consumer information taken home must be safeguarded.

Staff must not discuss consumers in public areas, including the reception area.

Staff must remove all consumer information from printers immediately.

Each care manager shall arrange for the security of the high risk consumer lists that accompany them when they are away from the office for use in emergencies.

The Information Technology Department is responsible for safeguarding the electronic record and its contents against loss, defacement, and tampering. IT is also responsible for safeguarding the records against use by unauthorized individuals or personnel.

Staff inputting consumer information into SAMS and other consumer record sites must have private passwords to enter the system. Monitors shall be directed away from the line of vision of the public or other personnel. SAMS screens must be minimized when computers are not in use; or the user must log out of SAMS. Direct service staff should be mindful that consumer information located on the Details screen of a SAMs consumer record is accessible to individuals outside of BSHC who have access to SAMs. Therefore, staff should never mention a consumer's involvement with Protective services and/or information about a difficult family member on the Details screen in SAMs.

Facsimile (FAX) transmissions of consumer information must be restricted in the same manner as written material in the case record. Use of the agency Fax cover sheet with confidentiality warning is required for all transmission with consumer information. Faxes must not be left unattended. Verifying the accuracy of Fax numbers of recipients is required.

All consumer information in any form on desks and bulletin boards must be locked in desks at the end of the day.

[86] EOEA PI-97-55

4. Complaints/Breaches[87]

The Privacy Official is responsible for documenting, investigating and responding to all consumer complaints regarding confidential healthcare information, and determining whether a breach has occurred. Any complaint regarding the privacy of confidential healthcare information is to be made in writing to the Privacy Official of BSHC.

In accordance with 45 Code of Federal Regulations (CFR) 164.402, Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information.

(1) (i) For purposes of this definition, compromises the security or privacy of the protected health information means poses a significant risk of financial, reputational, or other harm to the individual.

(ii) A use or disclosure of protected health information that does not include the identifiers listed at § 164.514(e)(2), date of birth, and zip code does not compromise the security or privacy of the protected health information.

(2) Breach excludes:

(i) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part.

(ii) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part.

(iii) A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Upon receiving the complaint regarding confidential healthcare information, the Privacy Official is to:

- Document the complaint in the Complaint Log.
- Document the date, time and name of person making the complaint in the Complaint Log.
- Investigate the complaint in accordance with 45 Code of Federal Regulations (CFR) 164.402 (see above definitions).
- Document the resolution of the complaint in the Complaint Log.
- Communicate the outcome of the complaint with the individual filing the complaint.

The Privacy Official will communicate the number of complaints and resolutions to senior management during bi-weekly senior staff meetings. This in house process outlined above does not retract an individual's right to file a complaint with the Secretary of Health and Human Services if they believe BSHC has not

[87] 45 CFR § 164.530(d)

complied with HIPAA regulations or if the problem was not resolved by the Privacy Official. BSHC will cooperate with any investigation resulting from such and shall provide access to information and records.

5. Sanctions[88]

BSHC will apply sanctions to employees failing to comply with the policies and procedures regarding the security and confidentiality of healthcare information.

If an employee is found to violate any policy or procedure in regards to confidential healthcare information the organization's policy on disciplinary action will be implemented.

The severity of discipline will be determined according to:

- The severity of the violation.
- If the violation was intentional or unintentional.
- If the violation indicates a pattern or practice of improper use or release of confidential healthcare information.

The degree of discipline may range from a verbal warning to termination. Each episode of employee discipline regarding confidential healthcare information is to be documented and reported to the Privacy Official.

6. Mitigation[89]

BSHC will attempt to mitigate any harmful effects from the misuse of protected healthcare information by the organization or any business associates. Once BSHC is notified that confidential healthcare information has been misused by an employee or business associate, this information shall be communicated to the Privacy Official. If an employee has misused the information, the policy on employee sanctions is to be implemented.

If the information has been misused by a business associate, the organization is to:

- Investigate the misuse of the information.
- Determine if the misuse was serious.
- Determine if the misuse is repeated.
- Counsel the business associate on the misuse of confidential healthcare information.
- Monitor the business associate's performance to ensure that the wrongful behavior has been remedied.

The organization reserves the right to terminate a business associate agreement in the event the misuse of confidential healthcare information continues despite counseling.

7. Documentation

All communications that are required by HIPAA or BSHC confidentiality policies shall be maintained in hard copy or electronic form by the Privacy Official. In addition, the Privacy Official shall maintain a written or

[88] 45 CFR § 164.530(e)
[89] 45 CFR § 164.530(f)

electronic record of any activity, designation, or action that HIPAA requires to be documented. Such documentation shall be retained for seven years from the date it was created or the date it was last effective, whichever is later.

V. APPENDICES

Appendix A: Business Associates Agreements

SERVICES FOR WHICH NO BUSINESS ASSOCIATE AGREEMENT IS REQUIRED	
Adult Day Health	Behavioral Health Services
Competency Evaluation	Alzheimer's Day Programs
Nutritional Assessment	Personal Emergency Response
Habilitation Therapy	Respite Care
Home Health Services (HHA, PT, OT, SN, Speech Therapy)	Supportive Day Programs
Homemaking/Personal Care	Supportive Homecare Aide
Medication Dispensing System	Vision Rehabilitation
	Wanderer Locator Service

SERVICES FOR WHICH **A BUSINESS ASSOCIATES AGREEMENT *MAY* BE REQUIRED**	
Transportation	No BAA required with a provider of medical transportation. BAA required with all others.
Environmental Accessibility Adaptations	No BAA required with providers of medical equipment or OT services that perform adaptive housing. BAA required will all others.
Emergency Shelter	No BAA required if the facility is a hospital, nursing home, or other facility whose services regularly include health services, such as personal care or PERS. BAA required for all others.

SERVICES FOR WHICH **A BUSINESS ASSOCIATES AGREEMENT IS REQUIRED**	
Chore	Legal Services
Companion	Financial Consultation Services
Laundry	Bill Payer Services
Grocery Shopping	Representative Payee
Home Delivered Meals	Translation/Interpreting

RELEASE OF INFORMATION AUTHORIZATION FORM

Boston Senior Home Care (BSHC) is requesting _____ (consumer) to authorize the use and disclosure of confidential healthcare information to (names and/or organizations) _____

for the following purposes: List and describe the specific purposes: _____

_____(Or write "At the request of the individual" in this space.) _____

The information will be released by (list person or class of persons who will make the disclosure) _____ to (list the person or class of persons to whom the disclosure will be made) _____.

List the specific information that is to be used: _____

_____

CONDITIONS:

- The consumer voluntarily agrees to authorize the above named individuals/organization to access his/her confidential healthcare information only for the purpose listed above.
- Once released, the information may no longer be covered under the federal privacy protection, and may be subject to re-disclosure.
- The consumer has the right to refuse to sign this authorization. If the consumer does not sign to give BSHC permission to release or he revokes permission, the consumer's home care services will not be affected.
- The consumer has the right to revoke this authorization at any time. This revocation must be writing to BSHC. (Any use or disclosure prior to revocation is valid and will not be affected by the revocation.)
- This authorization is in effect from _____ to _____ (length of time), or in the event that_____, whichever occurs first. Upon the conclusion of that time period, this authorization is automatically revoked and no further use of the consumer's confidential healthcare information is permitted beyond that date.

SIGNATURES: I have had the opportunity to read and consider the contents of this authorization. I confirm that the contents are consistent with my direction.

Consumer/Legal Representative: _____ Date: _____

Relationship or Authority of Personal Representative_____.

HIPAA Release Authorization 04/03: Original to record; copy to consumer

NOTICE OF PRIVACY PRACTICES

Boston Senior Home Care (BSHC) provides a variety of services that enable older people and adults with disabilities to stay at home in the community. Because we work with a variety of funding sources, including Medicaid, and get referrals from a number of health care providers, we may have personal health information about you.

Personal health information includes things such as certain medical diagnoses, the kinds of medical or treatment services you get, or the dates you get the services. This notice explains when BSHC may use and share your health information and your rights regarding your health information.

By law, BSHC must:

- *protect the privacy of your health information as described in this notice;*
- *explain our privacy practices to you; and*
- *notify you if your unsecured health information is obtained by an unauthorized person.*

BSHC may use or share your health information:

- when communicating with family members or other persons identified as a contact person for your care or your general condition;
- with medical professionals including: primary care physicians, other physician specialists and their office medical staff, local

hospitals, rehabilitation facilities, health insurances or nursing homes, as part of managing your care;

- when required by law;
- for payment activities, such as checking if you are eligible for health benefits, and being paid for services you get;
- to operate our programs, including evaluating the quality of the services you get;
- with our provider vendors to coordinate your services;
- with health-oversight agencies (such as the MassHealth, or the federal Centers for Medicare and Medicaid Services) for oversight activities authorized by law, including fraud and abuse investigations;
- for research projects that meet privacy requirements, and help us evaluate or improve the Agency's programs;
- with government agencies that give you benefits or services;
- to prevent or respond to an immediate and serious health or safety emergency;
- to tell you about new benefits and services, or health-care choices you have; and
- to raise funds for BSHC charitable purposes.

Except as described above, BSHC cannot use or share your health information with anyone without your written permission. You may cancel your permission at any time, as long as you tell us in writing. We must get your permission to use your information for marketing purposes or when we are paid for your health information. Please Note: We cannot take back any health information we used or shared when we had your permission.

You have the right:

- to see and get a copy of personal health information. You must ask for this in writing, or direct someone else that you designate to

write on your behalf. If you have someone acting as a Power of Attorney, Health Care Proxy Holder, Guardian or Conservator, he or she may also execute this document. BSHC may charge you to cover certain costs, such as copying and postage;

- to ask BSHC to change your health information if you think it is wrong or incomplete. You must tell us in writing, or direct someone else that you designate to write on your behalf. If you have someone acting as a Power of Attorney, Health Care Proxy Holder, Guardian or Conservator, he or she may also execute this document. Identify what health information you want us to change, and why;
- to ask BSHC to limit its use or sharing of your health information. You must ask for this in writing, or direct someone else that you designate to write on your behalf. If you have someone acting as a Power of Attorney, Health Care Proxy Holder, Guardian or Conservator, he or she may also execute this document. BSHC is not required to agree to your request, unless it relates to a service for that you have paid for in full;
- to ask BSHC to get in touch with you in some other way, if contacting you at the address or telephone number we have on file for you would put you in danger. Please let us know by telephone and tell us exactly where and how BSHC should contact you so that we may discuss. BSHC will confirm, in writing with you what you have stated.
- to get a list of when and with whom BSHC has shared your health information, with certain exceptions. You must ask for this in writing or direct someone else that you designate to write on your behalf. If you have someone acting as a Power of Attorney,

- Health Care Proxy Holder, Guardian or Conservator, he or she may also execute this document; and
- to ask BSHC not to solicit funds for BSHC for charitable purposes.
- to get a paper copy of this notice at any time.

By law, BSHC must give you this notice explaining that we protect your health information, and that we must follow the terms of this notice.

If we at BSHC change how we use and share your health information, we will notify you of these changes.

BSHC takes your privacy very seriously. If you would like to exercise any of the rights we describe in this notice, or if you feel that BSHC has violated your privacy rights, contact BSHC's Privacy Officer in writing at the following address:

Joanne McMahan
Privacy Officer
Boston Senior Home Care
89 South Street, Suite 501
Boston, MA 02111

Filing a complaint or exercising your rights will not affect your covered services. You may also file a complaint with the U.S. Secretary of Health and Human Services.

For more information, or if you need help understanding this notice, call (617) 303-8307 Monday through Friday, 9 a.m. – 5 p.m.

Effective: 9/1/2013
Replaces: 11/7/2011

Acknowledgement of Receipt of Privacy Notice

Consumer Name and Address:

_____
_____
_____

I have been given a copy of **(BSHC Name)** Notice of Privacy Practices that describes how my health information is used and shared. I understand that **(BSHC Name)** has the right to change this notice at any time.

Date:_____

_____ or _____

Signature of Consumer Representative

Signature of Consumer's

_____ _____

Printed Name

Printed Name

_____

Relationship to Consumer

Acknowledgement Refused:
Efforts to Obtain: _____
Reason for Refusal: _____