

**HIPAA Privacy Policy for the**

**ERISA Health Plans of**

**The Dow Chemical Company**

**And Union Carbide Corporation,**

**a subsidiary of The Dow Chemical Company**

**Original effective date: April 14, 2003**

**Amended and Restated: August 20, 2010**

I.	Introduction.....	1
	A. Purpose and Application .....	1
	B. Scope.....	1
	1. EPEP, A Hybrid Entity .....	2
	C. Maintenance and Amendment .....	2
	D. Privacy Official.....	2
	E. Health Plan Documents.....	3
	F. Other Dow Policies .....	3
	G. Effective Date .....	3
II.	Definitions.....	4
III.	Responsible Persons.....	11
	A. Privacy Official Appointed.....	11
	B. Responsible Persons.....	12
	C. Supervisors.....	12
IV.	Minimum Necessary Rule.....	13
	A. General Rule .....	13
	B. Criteria for Determining Minimum Necessary .....	13
	C. Exceptions to Minimum Necessary Requirement.....	13
	D. Reliance on Request for Information.....	14
	E. Routine Transactions .....	14
	F. Non-Routine Transactions .....	15
	G. Responsibility for Application of Minimum Necessary Requirement .....	16
V.	Safeguarding Protected Health Information .....	17
	A. General Rule .....	17
	B. Physical Security.....	17
	C. Electronic Security.....	18
	D. Security of Specific Materials and Communications.....	20
VI.	Permitted Health Plan Uses and Disclosures of Protected Health Information.....	25
	A. Uses and Disclosures for a Health Plan’s Own Payment, Treatment, or Health Care Operations .....	25
	B. Disclosures to Individuals.....	25
	C. Disclosures to Friends and Family Members.....	26
	D. Disclosures to a Health Care Provider for Treatment Purposes. ....	27
	E. Disclosures to a Dow Health Plan .....	27
	F. Disclosures to Another Dow or UCC Benefit Plan, Other than a Health Plan.....	28
	G. Disclosures to the Plan Sponsor and Employer .....	29
	H. Disclosures to Another Covered Entity or a Health Care Provider for Payment Purposes.....	30
	I. Disclosures to a Non-Dow Health Plan .....	31
	J. Uses and Disclosures for Health and Safety Purposes.....	31
	K. Uses and Disclosures Pursuant to Legal Proceedings and Law Enforcement .....	33

L.	Uses and Disclosures Concerning Decedents .....	35
M.	Uses and Disclosures for Other Government Purposes .....	36
N.	Disclosures to U.S. Department of Health and Human Services.....	37
VII.	Uses and Disclosures Only With Authorization .....	38
A.	Authorization Required.....	38
B.	Required Elements for a Valid Authorization .....	38
C.	Authorization as a Condition of Enrollment.....	38
D.	Revocation of an Authorization .....	39
E.	Recordkeeping .....	39
VIII.	Individuals' Rights Regarding Protected Health Information .....	40
A.	Privacy Notice.....	40
B.	Access to Protected Health Information .....	40
C.	Request for Restriction on Uses and Disclosures .....	42
D.	Request for Alternate Address/Confidential Communication .....	43
E.	Amendment of Protected Health Information.....	43
F.	Accounting.....	45
G.	Complaints .....	46
H.	Personal Representatives .....	47
IX.	Business Associates .....	48
A.	Obligations of Business Associates .....	48
X.	Health Plan Privacy Administration .....	49
A.	Written Policy .....	49
B.	Enforcement of Privacy Policy .....	49
C.	Employee Training.....	50
D.	Recordkeeping Activities.....	51
XI.	Routine Health Plan Transactions.....	52
A.	Resource Center .....	52
B.	HR Service Center and Retiree Service Center .....	54
C.	Payroll.....	55
D.	Information Systems .....	55
E.	Internal Auditors .....	55
F.	Strategic Center.....	55
G.	Legal .....	56
H.	Pension/Retirement Counseling.....	56
I.	Records Retention Center .....	56
J.	Health Services Department .....	56
K.	Global Reporting Team.....	57
L.	Retirement Board.....	57

XII.	Security of Electronic PHI .....	58
A.	Introduction.....	58
B.	Integration with Other Dow Policies .....	58
C.	Administrative Safeguards.....	58
D.	Physical Safeguards .....	63
E.	Technical Safeguards .....	65

Exhibit A: Notice of Privacy Practices

Exhibit B: Privacy Official and Responsible Person Delegations

Exhibit C: Routine Disclosures to Business Associates

Exhibit D: Areas Where Access Is Restricted to Responsible Persons

**HIPAA Privacy Policy for the  
ERISA Health Plans  
of The Dow Chemical Company  
and Union Carbide Corporation,  
a subsidiary of The Dow Chemical Company**

**I. Introduction**

**A. Purpose and Application**

This HIPAA Privacy Policy (Privacy Policy or Policy) reflects practices that have been adopted by The Dow Chemical Company and Union Carbide Corporation, a subsidiary of The Dow Chemical Company, on behalf of their Health Plans to protect the privacy of Health Plan participants' health information. The Privacy Policy is intended to comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) as it pertains to health care privacy and certain electronic transactions.

The United States Department of Health and Human Services (HHS) issued complex HIPAA privacy regulations referred to as the Privacy Rule. If any provision of this Policy is inconsistent with HIPAA or a more restrictive applicable state privacy law, the Policy will be interpreted to comply with such law.

**B. Scope**

The Dow Chemical Company and Union Carbide Corporation, a subsidiary of The Dow Chemical Company, as Health Plan sponsors, maintain their commitment to safeguard and keep confidential the individual health information of their employees and their families. Consistent with the requirements of the Privacy Rule, any Protected Health Information (PHI) received by, or on behalf of a Health Plan may be used or disclosed solely in accordance with this Privacy Policy.

The following plans (as amended from time to time) are covered by this Policy:

- The Dow Chemical Company Medical Care Program
- The Dow Chemical Company Dental Assistance Program
- The Dow Chemical Company Health Care Reimbursement Account
- The Dow Chemical Company Executive Physical Examination Program (health care component only)
- The Dow Chemical Company Retiree Medical Care Program
- The Dow Chemical Company Retirement Health Care Assistance Plan (RHCAP)
- The Dow Chemical Company Insured Health Program

- Union Carbide Corporation Retiree Medical Care Program
- Union Carbide Corporation Insured Retiree Health Program
- Rohm And Haas Company Health and Welfare Plan

However, for health benefits offered under an insured arrangement or through a health or dental maintenance organization (HMO or DMO), this Privacy Policy will not apply to the extent that the privacy policy of the respective health insurance issuer or HMO or DMO applies. That is, to the extent that the privacy policy of the respective health insurance issuer or HMO or DMO addresses the situation, such privacy policy of the insurer or HMO or DMO will apply instead of the Dow or UCC Health Plan Privacy Policy. Individual health information provided to Dow by or on behalf of an employee in connection with verifying an absence from employment, request for a reasonable accommodation of a disability, workers compensation claim, or other employment-related purpose, is not subject to this Privacy Policy.

#### 1. EPEP, A Hybrid Entity

Dow's Executive Physical Examination Program (EPEP) is a hybrid entity, as defined under HIPAA. EPEP is only available to certain executives. EPEP is a health plan covered under the Privacy Rule, however, only the "health care component" is covered under the Privacy Rule requirements. Generally, the "health care component" of EPEP is the portion of EPEP that administers the enrollment and eligibility rules of EPEP, communicates the medical coverage available under EPEP, makes claims determinations, and pays claims. The EPEP "health care component" does not include medical consultation or scheduling of medical appointments. This Privacy Policy only applies to the health care component of EPEP.

The "Non-health care component" of EPEP schedules medical appointments and provides medical consultation. The "Non-health care component" also may request copies of the executive's medical records and keep them on file. This part of EPEP is not subject to the Privacy Policy.

Except as otherwise provided by the Privacy Rule, Protected Health Information (PHI) held by the "health care component" generally may not be disclosed to the "non-health care component" of EPEP (or anyone else) without authorization of the patient. Note that the Privacy Rule does allow the EPEP "health care component" to disclose enrollment and disenrollment information and Summary Health Information to the employer without an employee's authorization. In addition, the Privacy Rule also allows the EPEP "health care component" to disclose PHI to a health care provider for purposes of treating the patient.

#### **C. Maintenance and Amendment**

Any questions about this Policy should be directed to the Privacy Official.

#### **D. Privacy Official**

This Privacy Policy is the responsibility of the Privacy Official, who may amend it in any respect as he or she deems necessary or appropriate from time to time, with the approval of the Vice President - Human Resources.

#### **E. Health Plan Documents**

The plan documents for each of the Health Plans will be amended to address the Privacy Rule requirements. The Health Plans may be further amended as necessary or appropriate to reflect changes in this Policy.

#### **F. Other Dow Policies**

This Privacy Policy should be read in conjunction with and as a complement to Dow's security policies, including such policies as emergency services and security policies, computer password security policy, e-mail security policy and other policies, many of which are posted on Dow's IntraNet. See also "Policy on Protection of Personal Employee Data" on the Dow IntraNet. See Article XII. B. for a list of IS security policies. The Privacy Official is responsible for resolving any conflicts between the terms of this Privacy Policy and any other Dow policy.

#### **G. Effective Date**

The Privacy Policy was first effective April 14, 2003, and may be amended from time to time. The amendments shall be effective as of the date stated on the amendment, or if the Policy is restated, the effective date of the restatement.

## II. Definitions

- Authorization – an Individual’s specific written permission, as described in Policy Article VII, allowing a Health Plan to use and disclose PHI for purposes other than Payment, Health Care Operations, or one of the purposes described in Policy Articles VI B- through -N.
- Business Associate – a person or entity, other than a Dow or Health Plan employee, who performs or assists in the performance of a function or activity involving the use or disclosure of PHI from or on behalf of a Health Plan. Such functions or activities include claims processing or administration, data analysis, utilization review, quality assurance, billing, benefit management, repricing, and other professional services. “Business Associate” will include all employees of the Business Associate who perform or assist in the performance of functions on behalf of a Dow Health Plan.
- Claims data or information – Any category of data that the Plan Administrator of the applicable Health Plan generally needs to determine whether claims for plan benefits or claims for eligibility determinations should be approved or denied under the applicable Health Plan, and to process such claims. In addition, Claims Data includes any data resulting from the decision to pay or deny the claim. The data that comprises Claims Data may consist of PHI, and may consist of data or information that is not PHI. Claims data may also include Eligibility Data.
- Company - The Dow Chemical Company.
- Covered Participant - an Individual participating in a Health Plan based on his or her status as a current or former Dow employee, a surviving dependent of a former Dow employee, a beneficiary of a qualified medical child support order (QMCSO), or a person entitled to continuation coverage pursuant to the Consolidated Omnibus Budget Reconciliation Act of 1985 (COBRA).
- Covered Entity - means a health plan, a health care clearinghouse, or a Health Care Provider who transmits any health information in electronic form in connection with a Transaction covered by HIPAA.
- De-identified Information - health information that does *not* include any of the following identifiers of the Individual or the Individual’s relatives, employers, or household members: name, geographic subdivision smaller than a state, month and day of birth and other personal dates, telephone number, fax number, electronic mail address, social security number, medical record number, health plan beneficiary number, account number, certificate or license number, vehicle identifier (including serial or license plate number), device identifier, serial number, Web universal resource locator, Internet protocol address number,

biometric identifier, full face photographic image, or any other unique identifying number, characteristic, or code.

Health information is also De-identified Information if a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; provided that the results of the analysis that justify such determination are documented by such person.

- Designated Record Set – a record that includes PHI maintained by or for a Health Plan that pertains to enrollment, payment, claims adjudication, medical or case management, and other information used to make Health Plan related decisions about Individuals.
- Dow – The Dow Chemical Company and certain of its subsidiaries.
- Electronic PHI (“ePHI”) – PHI that is transmitted by or maintained in electronic media, as defined under 45 CFR s. 160.103.
- Electronic Transmissions - includes transactions using all forms of electronic media. Such transactions include the transfer of information over the Internet (wide-open), Extranet (using Internet technology to link a business with information only accessible to collaborating parties), leased lines, dial-up lines, and private networks. Electronic media includes magnetic tape, disk or compact disc media. Telephone voice response and “faxback” (a request for information made via voice using a fax machine and requested information returned via that same machine as a fax) systems and facsimile transmissions are not included.
- Eligibility data or information– any category of data that the Plan Administrator of the applicable Health Plan generally needs to determine whether a person or persons, is or are, eligible to participate in the applicable Health Plan. Eligibility Data also includes data that the Plan Administrator needs to administer the provisions of the Health Plan. Depending on the Health Plan, such information may include, but is not limited to: name, names of dependents, address, gender, date of birth, salary, dependent status (i.e. spouse, domestic partner, natural child, adopted child, step-child), employment status (i.e. retired, active, bargained for, LTFT, leave of absence), spouse employment status, proof of dependent status.
- Enrollment data or information – categories of data that the applicable Plan Administrator may use to determine the kind of coverage or benefits participants have under a particular Health Plan. Such information may include, but is not limited to: type of plan, names of dependents, plan option, levels of coverage, premiums or contribution amounts, payment options and amounts.

- He, him or his – all references to the masculine are intended to be gender-neutral and refer to either the masculine or feminine gender.
- Health Care – means care, services, or supplies related to the health of an individual, as “health care” is defined in 45 CFR. 160.103.
- Health Care Operations – any of the following activities to the extent that they are related to a Health Plan’s covered functions:
  1. Conducting quality assessment and improvement activities; population-based activities related to health improvement, reduction of health care costs, case management and care coordination, contacting Health Care Providers and patients regarding treatment alternatives; and related functions that do not include treatment;
  2. Reviewing competence or qualifications of health care professionals, and evaluating provider and Health Plan performance;
  3. Underwriting and other activities that relate to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance);
  4. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
  5. Business planning and development, such as cost-management and planning-related analysis related to managing and operating a Health Plan, and development or improvement of coverage policies; and
  6. Business management and general administrative activities including but not limited to: (i) management activities related to implementation of and compliance with the requirements of the Privacy Rule, (ii) customer service, including the provision of data analyses for Dow, provided that PHI is not disclosed to Dow; (iii) resolution of internal grievances, (iv) due diligence in connection with the sale, transfer, merger, or consolidation of all or part of a Health Plan with another Covered Entity or an entity that, following such activity, will become a Covered Entity, and (v) consistent with applicable requirements of the Privacy Rule, creating De-identified Information or a limited data set.
- Health Care Provider - a person or entity that provides, bills for, and/or is paid for providing medical or health services, as defined in 45 CFR § 160.103.
- Health Plan – each of the employee benefit programs that is sponsored by The Dow Chemical Company or Union Carbide Corporation that provide health care benefits

for employees, former employees, and dependents, including: medical, retiree medical, dental, employee assistance, and flexible spending account programs. The Health Plans are listed in Article I B.

- HHS - The United States Department of Health and Human Services, the agency charged with interpreting and enforcing the Privacy Rule.
- HIPAA – the Health Insurance Portability and Accountability Act of 1996 (as amended), and the regulations promulgated thereunder.
- HIPAA Security Policy -- Article XII of the Privacy Policy, entitled “Security of Electronic PHI”.
- H.R. Service Center – the portion of the Company’s Human Resources Department responsible for fielding questions from employees and others regarding the Health Plans. Calls may be answered by HR Service Center personnel or referred to Resource Center or Strategic Center subject matter experts or applicable third party vendors administering the applicable health plan.
- Individual – a person covered by a Health Plan or a decedent previously covered by a Health Plan who is the subject of the PHI.
- Information Systems Department (“IS”) – the part of Dow that is responsible for providing computer software and hardware services to Dow.
- Limited Data Set – PHI that excludes the direct identifiers listed in the Privacy Rule, but still contains some individually identifying information. 45 CFR s. 164.514 (e)(1).
- Minimum Necessary - the standard described in Article IV of this Privacy Policy to limit PHI that is accessed, requested, used, disclosed, created, or transmitted in accomplishing Payment, Health Care Operations, and other functions of the Health Plan.
- Notice - a written description of the Health Plans’ uses and disclosures of Individuals’ PHI that satisfies the requirements of and is distributed in accordance with 45 C.F.R. 164.520. A copy of the current Notice is appended as Exhibit A.
- Payment – activities undertaken by a Health Plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits, including but not limited to:
  - Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;

- Risk adjusting amounts due based on enrollee health status and demographic characteristics;
  - Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;
  - Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;
  - Utilization review activities, including precertification and preauthorization of services, and concurrent and retrospective review of services; and
  - Disclosure to consumer reporting agencies of necessary information relating to collection of premiums or reimbursement.
- Personal Representative - a person entitled under applicable law to decide and act on behalf of an Individual with respect to the Individual's health care. For example, parents of minor children and court-appointed guardians generally are Personal Representatives, except as otherwise explained in this Policy. (See Policy Article VIII H. The executor, administrator, or other person with authority to act on behalf of a deceased Individual's estate will be treated as the deceased Individual's Personal Representative. A Personal Representative is entitled to act on behalf of the Individual under the Privacy Policy.
  - Plan Sponsor – the Plan Sponsor of the following Health Plans is The Dow Chemical Company: The Dow Chemical Company Medical Care Program; The Dow Chemical Company Dental Assistance Program; The Dow Chemical Company Health Care Reimbursement Account Plan; The Dow Chemical Company Executive Physical Examination Program; The Dow Chemical Company Insured Health Program; The Dow Chemical Company Retiree Medical Care Program; The Dow Chemical Company Retirement Health Care Assistance Plan (“RHCAP”); Rohm and Haas Company Health and Welfare Plan. The Plan Sponsor of the following Health Plans is Union Carbide Corporation: Union Carbide Corporation Retiree Medical Care Program; Union Carbide Corporation Insured Retiree Health Program.
  - Privacy Official– the person designated by the Company and by Union Carbide Corporation responsible for implementing and updating the Privacy Policy and for carrying out the duties assigned to him or her under the Privacy Policy. Reference to the Privacy Official includes any person(s) to whom the Privacy Official has made an applicable delegation.
  - Privacy Policy – HIPAA Privacy Policy for ERISA Health Plans of The Dow Chemical Company and Union Carbide Corporation, a subsidiary of The Dow Chemical Company.

- Privacy Rule - the provisions of HIPAA which address health information privacy and security.
- Protected Health Information (PHI) – individually identifiable health information that (a) relates to the past, present, or future physical or mental condition of an Individual, provision of health care to an Individual, or payment for such health care; (b) can either identify the Individual or there is a reasonable basis to believe the information can be used to identify the Individual; and (c) is received or created by or on behalf of a Health Plan.
- Qualified Protective Order – an order of a court or an administrative tribunal or a stipulation by the parties that prohibits the parties from using or disclosing PHI for purposes other than the underlying litigation or proceeding for which the records are requested and requires the return to a Health Plan or destruction of the PHI at the end of the litigation or proceeding.
- Resource Center - the portion of the Company’s Human Resources Department responsible for the Health Care Operations, and to a lesser extent the Payment activities, for the Health Plans.
- Responsible Person – an employee of Dow whose duties (a) require that the employee have access to PHI for purposes of Health Plan Payment or Health Care Operations, or (b) make it likely that he or she will receive or have access to PHI. Persons designated as Responsible Persons are described in Article III. Any other employee who receives PHI from or on behalf of the Health Plan, even though his or her duties do not (or are not expected to) include receiving PHI, will be treated as a Responsible Person under the Privacy Policy, and will be referred to as a “Responsible Person”. In addition, employees of Business Associates who have access to Dow’s Global Human Resource Information System are also Responsible Persons. See Exhibit B regarding Level I or Level II Responsible Person designations.
- Retiree Service Center – a group of persons employed by a business associate responsible for fielding questions from retirees and others regarding the retiree Health Plans. Calls may be answered by Retiree Service Center personnel or referred to Resource Center subject matter experts or applicable third party vendors administering the applicable health plan.
- Retirement Board – the Retirement Board of The Dow Chemical Company.
- RHCAP – The Dow Chemical Company Retirement Health Case Assistance Plan.
- Security Official – the Security Official is the same person as the Privacy Official. The Security Official is responsible for insuring that the provisions of the Privacy Policy comply with 45 CFR Part 164.

- Security Regulations – 45 CFR Part 164.
- Social Security number – an individual’s social security number is considered Protected Health Information under this Privacy Policy.
- Strategic Center - the portion of the Company’s Human Resources Department responsible for design activities and certain plan administrative aspects of the Health Plans.
- Summary Health Information – information that may be individually identifiable health information, and summarizes the claims history, claims expenses, or type of claims experienced by individuals for whom a plan sponsor has provided health benefits under a group health plan; and from which most identifying information has been deleted as specified in 45 CFR s. 164.504(a).
- Transaction – the transmission of information between two parties to carry out financial or administrative activities as related to Health Care, as “transaction” is defined in 45 CFR s. 164.103.
- Treatment – 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; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another. Except for some aspects of the medical component of the Employee Assistance Program (EAP), Dow’s and Union Carbide’s Health Plans do not provide Treatment.
- Vice President, Human Resources – the Vice President of Human Resources for the Company. By authority of the Resolution of the Board of Directors of Union Carbide Corporation dated as of February 6, 2001, the Vice President of Human Resources of The Dow Chemical Company is authorized to act on behalf of Union Carbide Corporation with respect to the Union Carbide Corporation Health Plans and to act on behalf of the Union Carbide Corporation Health Plans.
- Visitor – a person who is not an employee of Dow.

### **III. Responsible Persons**

#### **A. Privacy Official Appointed**

The Privacy Official for the Health Plans is the individual appointed by the Vice President - Human Resources and is listed in Exhibit B. The Privacy Official is responsible, and has the authority, for:

1. amending, implementing, and updating this Privacy Policy;
2. providing and documenting appropriate privacy training for Responsible Persons;
3. investigating and responding to Individuals' complaints regarding possible impermissible uses or disclosures of PHI and related Policy violations;
4. investigating and responding to reports by Responsible Persons and other employees regarding possible impermissible uses or disclosures of PHI and related policy violations or improvements;
5. providing Individuals with a Notice and information regarding this Privacy Policy; and
6. providing Individuals with access to inspect and copy their PHI maintained in a Designated Record Set (See Article VIII B);
7. accepting and responding to requests for restriction of a Health Plan's use or disclosure of an Individual's PHI (See Article VIII C);
8. accepting and responding to requests for communication of PHI by alternative means or alternative locations (See Article VIII D);
9. accepting and responding to requests to amend PHI maintained in a Designated Record Set (See Article VIII.E);
10. accepting and responding to requests for an accounting of disclosures of PHI (See Article VIII.F);
11. maintaining documentation of the Privacy Policy, Notices, complaints, and related activities consistent with the recordkeeping procedures in this Privacy Policy (See Article X.D);
12. obtaining, negotiating, and signing contracts with Business Associates, and investigating and responding to Business Associate compliance concerns (See Article IX). The applicable Plan Administrator for the Health Plans and the Plan Sponsor may also sign contracts with Business Associates; and
13. maintaining PHI security documentation (See Article V).

The Privacy Official may delegate any of his or her responsibilities under the Privacy Policy.

## **B. Responsible Persons**

The Health Plans are currently administered by Business Associates and employees within the HR Service Center, Resource Center, Strategic Center, Information Systems, Accounting/Payroll, Employee Data Resource Center (EDRC), Retiree Service Center, and Health Services function (with respect to the Executive Physical Examination Program only). The Dow Chemical Company Retirement Health Care Assistance Plan (“RHCAP”) is also administered by the Retirement Board.

The persons listed by job title or job class in Exhibit B are Responsible Persons. Additional job titles or job classes may be designated as Responsible Persons with the approval of the Privacy Official.

Under certain circumstances, it may be necessary for an employee who is not normally a Responsible Person to have access to PHI. This could occur, for example, when an employee is assigned to temporarily replace a Responsible Person who is out on vacation. In these situations, the employee is treated as a Responsible Person for purposes of this Privacy Policy and may have access to, or receive, record, and/or transmit PHI either (a) at the direction of, or under the supervision of, a Responsible Person, or (b) where such access is necessary to support the services provided by a Responsible Person. In all other cases, however, a non-designated Responsible Person should avoid contact with PHI when possible, unless the PHI relates directly to that employee as an Individual or the employee has been authorized (in accordance with Article VII) to use or receive the PHI.

## **C. Supervisors**

An employee who supervises a Responsible Person may receive or have access to PHI when necessary to assure that the Responsible Person is properly executing his or her job functions involving such PHI. Such a supervisor is treated as a Responsible Person for purposes of such receipt and access of PHI.

#### **IV. Minimum Necessary Rule**

##### **A. General Rule**

When using, disclosing, or requesting PHI to or from any person, the Responsible Person or Business Associate will make reasonable efforts to use, disclose, or request only the Minimum Necessary amount of PHI to achieve the particular purpose.

In addition to limiting the PHI used or disclosed, a Responsible Person or Business Associate must take steps to ensure that only the person(s) needing the PHI for the intended purpose receives it. This duty applies regardless of whether such recipients are other Responsible Persons, Business Associates, or other persons to whom the Responsible Person or Business Associate is required, permitted or authorized to disclose PHI. If a Responsible Person or Business Associate is the recipient of PHI, that employee should process, copy, or record such PHI without disclosing it to others, unless such disclosure is necessary.

Prior to any disclosure of PHI, the Responsible Person or Business Associate must verify the identity and authority of the person requesting such information, if not already known to the Responsible Person or Business Associate.

##### **B. Criteria for Determining Minimum Necessary**

The following criteria apply in determining whether a proposed Transaction involving PHI complies with the Minimum Necessary requirement:

- whether the intended use of the PHI is necessary for Payment, Health Care Operations, or another permitted function under Article VI to which the Minimum Necessary rule applies;
- whether the intended purpose could be served adequately if fewer people were permitted access to (*e.g.*, to use or receive disclosure of) the PHI;
- whether the intended purpose could be served adequately if less PHI is used or disclosed; and
- whether the method for transmitting the PHI ensures that it is received only by the intended recipient.

##### **C. Exceptions to Minimum Necessary Requirement**

The Minimum Necessary rule does not apply to the following Transactions:

- disclosure to a Health Care Provider for treatment purposes;
- disclosure to the Individual;
- disclosures to the Secretary of Health and Human Services ;

- uses and disclosures required by law ; and
- uses and disclosures for which the Individual has given Authorization .

**D. Reliance on Request for Information.**

A Responsible Person or Business Associate may assume that a third party's request for disclosure of PHI satisfies the Minimum Necessary rule if such reliance is reasonable under the circumstances and at least one of the following applies:

- the disclosure is to a public official who represents that the information requested is the Minimum Necessary for the stated purpose(s);
- the information is requested by another Covered Entity; or
- the information is requested by a Responsible Person or Business Associate, who is a professional, for the purpose of providing professional services to the Health Plan, and there is a representation that the information requested is the Minimum Necessary for the stated purpose(s).

**E. Routine Transactions**

1. Routine Transactions by Responsible Persons

Transactions performed by the Responsible Persons on a routine and recurring basis are documented in Article XI ("Routine Health Plan Transactions") and Exhibit C ("Routine Disclosures to Business Associates"). These routine transactions have been found to satisfy the Minimum Necessary requirement.

Prior to approving a routine Transaction involving PHI (*e.g.*, enrollment, premium collection and payment, and change-in-status notification), the Level I Responsible Person must:

- Review the process used by Dow for the use and disclosure of the particular PHI.
- Determine whether non-identifiable information can accomplish the intended purpose. If non-identifiable information can be used, then use the de-identified information instead of the PHI. If only PHI can accomplish the purpose, then continue to the next step.
- Determine whether the purpose of the use or disclosure of the PHI is for payment or treatment purposes, or health care operations. If the purpose is not for payment, treatment or health care operations, an authorization is needed to use or disclose the PHI. If the purpose is for payment, treatment or health care operations, then continue to the next step.

- If the purpose is for payment or treatment purposes, or health care operations, ascertain the minimal amount of PHI that is needed to accomplish the intended purpose. Make sure that the Dow process only allows the use and disclosure of this minimal amount of PHI.
- Determine the minimum number of Responsible Persons or Business Associates needed to accomplish the intended purpose. Make sure the Dow process only allows the use and disclosure only to these Responsible Persons or Business Associates.

2. Routine Transactions by Business Associates.

Business Associates will review Transactions performed on behalf of the Health Plans on a recurring basis for compliance with the Minimum Necessary rule. Business Associates will review the process by which the PHI is used or disclosed in the course of such routine transactions, and will provide evidence that such routine transactions comply with HIPAA to the Dow or the Health Plans upon request.

**F. Non-Routine Transactions**

1. Non-Routine Transactions by Responsible Persons.

A Responsible Person may make the decision to use or disclose PHI in a non-routine Transaction based on the following methodology:

- Determine whether the non-identifiable information can accomplish the intended purpose. If non-identifiable information can be used, then no PHI should be used or disclosed. If only PHI can accomplish the purpose, then continue to the next step.
- Determine whether the purpose of the use or disclosure of the PHI is for payment or treatment purposes, or health care operations. If the purpose is not for payment, treatment or health care operations, an authorization is needed. If the purpose is for payment, treatment or health care operations, then continue to the next step.
- If the purpose is for Payment or Treatment, or Health Care Operations, ascertain the minimum amount of PHI that is need to accomplish the intended purpose. Only use or disclose the minimum amount necessary.
- Determine the minimum Responsible Persons or Business Associates needed to accomplish the intended purpose. Only these people should use or disclose the PHI.

The Responsible Person should consult a Level I Responsible Person if he or she has any questions or concerns. (See Exhibit B).

2. Non-Routine Transactions by Business Associates.

Business Associates will review non-routine transactions performed on behalf of the Health Plans such as to comply with the Minimum Necessary rule, except where the Minimum Necessary rule does not apply (see Article IV C.).

### **G. Responsibility for Application of Minimum Necessary Requirement**

The Responsible Person or Business Associate who engages in a Transaction involving PHI is responsible for confirming that the Transaction meets the Minimum Necessary requirements. A Responsible Person may assume that a routine Transaction in a form approved by the appropriate Responsible Person at Level I or above meets these requirements. Nonetheless, if the Responsible Person has reason to believe that, under the particular circumstances, this is not the case, the Responsible Person should use his or her own judgment, based on HIPAA Privacy Policy, HIPAA Notice, and his or her training. The Responsible Person should consult the Privacy Official as needed for advice.

## **V. Safeguarding Protected Health Information**

### **A. General Rule**

A Responsible Person or Business Associate is permitted to access, receive, use, and/or transmit PHI for the purposes set forth in Article VI. When accessing, receiving, using and/or transmitting PHI, however, the Responsible Person or Business Associate must take reasonable steps to safeguard the PHI and keep it confidential, and to ensure that it is not intentionally or unintentionally used or disclosed for a purpose, or in a manner, inconsistent with this Privacy Policy.

Any breach of this Article V will be reported to the Privacy Official who will (1) act as necessary to maintain the security of any PHI, (2) take such action as he or she deems appropriate to prevent any similar breach in the future; and (3) impose appropriate sanctions against the Responsible Person or Business Associate accountable for the breach.

If the Privacy Official (or his or her designee) determines that sanctions against the Responsible Person causing such breach are warranted, he or she will consult with the Responsible Person's supervisor and will issue sanctions. All sanctions issued for a breach of this Policy, and any applicable sanctions and actions taken to prevent similar breaches, will be documented by the Privacy Official.

### **B. Physical Security**

PHI in physical form (*e.g.*, printed material, notes, computer disks and other physical storage media) will be maintained and stored by the Health Plan on the Dow's premises and/or on the premises of a Business Associate which has entered into an agreement with the Health Plan (or Plan Sponsor) and has certified that it maintains appropriate safeguards of PHI comparable to, or at least as stringent as those set forth below.

#### **1. Building Access**

Access to premises on which PHI is maintained or stored will be restricted. Persons regularly employed on the premises will be issued and display electronic or photographic "key cards" that permit the tracking of access into the building. Key cards, pass keys or other means of access will be issued and maintained in accordance with Dow's building security policies. Visitors entering the building will be required to sign in and show valid identification to building security personnel in accordance with Dow's building security policies. Entry will be denied to any person who does not have legitimate business on the premises.

#### **2. Access to Premises where PHI is Maintained or Stored**

In addition to the building security measures described above, access to the Resource Center premises and to other offices within a building where PHI is maintained or stored will be further restricted by keeping all doors locked (subject to fire safety requirements), so that a key card, pass key, numeric code or other means of access is required for entry. Where such restricted access is not possible, the PHI maintained or stored on the premises in physical form must be placed in a locked file cabinet at all times when not being used, in accordance with

paragraph 3 below. Entry to the Resource Center premises or other offices where PHI is maintained or stored will be restricted to Responsible Persons and, where appropriate, other employees of Dow who have legitimate business on the premises. An employee who is regularly authorized to access such premises (other than as a Visitor under the supervision of a Responsible Person, as described below) will be treated as a Responsible Person and will be trained on maintaining the security of PHI in accordance with Article VI. Dow Security will maintain a log of persons holding a key card, pass key, numeric code or other means of access to the premises where PHI is stored or maintained. A Responsible Person who lends a key card, pass key, numeric code or other means of access to any other person who is not a Responsible Person may be subject to sanctions under the Privacy Policy. Temporary pass keys or magnetic cards, etc. must be obtained from Dow Security. Any lost pass key or magnetic card must be reported to Dow Security, who will act as necessary to safeguard the premises, which (depending upon the circumstances) may include changing internal locks.

Visitors will be reported in advance to building security in accordance with Dow's physical security policies. A list of Visitors to the Resource Center will be maintained in a log. A Visitor will be permitted to enter premises in which PHI is maintained or stored only if he or she (1) is known to have legitimate business on the premises and (2) will be supervised on the premises by one or more Responsible Persons. Employees will promptly report to building security any person on the premises who does not display a valid identification pass for the premises.

Upon termination of a Responsible Person, or upon a change or reassignment of an employee whose job functions have changed so that he or she is no longer a Responsible Person, he or she shall be removed from authorized entry into the Resource Center premises or other offices where PHI is maintained or stored (and, if applicable, the building) and immediately surrender any pass key or magnetic card, etc. to the premises. With respect to a Responsible Person with access to the Global Human Resources Information System (GHRIS), the change or reassignment shall be reported through GHRIS, and authorized entry will be added or removed as appropriate. With respect to a Responsible Person who does not have access to GHRIS, the Privacy Official or his delegee will regularly check the list of those with authorized access to determine whether authorized access should be added or removed.

### 3. Protection of PHI Stored in Physical Form

When not required to be readily available for use by a Responsible Person, PHI maintained in physical form must be stored in a locked filing cabinet, office or similar repository, or secured in an area with restricted access to Responsible Persons. Areas with restricted access to Responsible Persons are listed in Exhibit D.

#### **C. Electronic Security**

PHI in electronic form (*e.g.*, e-mail, databases and computer files containing PHI) will be maintained and stored in a secure manner by the Health Plan and/or by a Business Associate which has entered (or will have entered by April 14, 2004) into an agreement with the Health Plan and has certified that it maintains appropriate safeguards of PHI that are comparable to, or at least as stringent as those set forth below. Electronic Transmissions containing PHI must, to

the extent reasonably possible, be protected so that they cannot be intercepted by parties other than the intended recipient, or accessed by unauthorized users.

See also Article XII, which addresses the storage and transmission of electronic PHI. Article XII is intended to comply with 45 CFR Part 164 (“Security Regulations”)

1. Access to Electronic PHI

Access to PHI in electronic form will be restricted to Responsible Persons. Responsible Persons whose job duties do not require use or disclosure of PHI, but who are located in areas where PHI is kept or have access to PHI through the Dow Global Human Resources Information System (GHRIS), must be trained not to look at, or use or disclose PHI. Failure to comply with this requirement may subject such Responsible Person to disciplinary action up to and including termination of employment.

Responsible Persons who need to access PHI in the normal course of their duties may access such electronic PHI only on authorized computers in accordance with the Dow’s electronic security policy. Each such computer will be assigned and maintained in accordance with the Dow’s policy on personal computers, including applicable procedures regarding password protection, periodic back-up, virus protection, etc. All computer files and databases containing PHI received, created or maintained by the Health Plan in electronic form which require access by more than one Responsible Person or which may be accessed by a Business Associate or Covered Participant will be maintained on a secure network, and all Dow security, firewall, data back up, access authorization and other policies and security procedures applicable to confidential material on a Dow extranet network will apply. Access to files, databases and other PHI in electronic form will be password protected and will be available only to Responsible Persons who have been trained as to their HIPAA privacy requirements.

In some cases it may be necessary to create a temporary or “working” file containing PHI, such as a word processing file or internal e-mail explaining resolution of a Health Plan claim. The Responsible Person will delete such files in accordance with the Dow’s Records Management Policy when no longer in use; or, if the file is part of the Designated Record Set or otherwise appropriate to retain, it will be stored on diskette or similar medium in accordance with these Privacy Policies. Upon termination of a Responsible Person, or upon a change or reassignment of an employee whose job functions have changed so that he or she is no longer a Responsible Person, he or she shall be removed from authorized entry into any files, databases and other PHI maintained in electronic form. Such terminations shall be reported to the Information Systems Department, who will remove the terminated employee’s authorized access.

Besides the Responsible Person in the Information Systems Department who routinely have access to PHI as a part of their job responsibilities, employees in the Information Systems Department may have access to files, databases and other PHI in electronic form for security and systems maintenance purposes. Such employees will be treated as Responsible Persons for purposes of Article V of the Privacy Policy and will be trained on maintaining the security of PHI in accordance with Article X.C. Any outside entity who is retained to perform information technology services will be required by contract to only access files, databases and other PHI in

electronic form, to the extent necessary to perform the services for which they were contracted to perform, and to only use and disclose such information as permitted under HIPAA.

## 2. Electronic Transmissions

A Responsible Person who performs Electronic Transmissions as part of his job functions, or a Business Associate contracted to perform Electronic Transmissions on behalf of a Health Plan, may engage in a Transaction involving the Electronic Transmission of PHI if the following conditions are met:

- The Responsible Person or Business Associate has determined that the Transaction is permitted under Article VI of the Privacy Policy;
- The Responsible Person or Business Associate has received reasonable assurances that the intended recipient has appropriate control of and access to the computer(s) receiving the Electronic Transmission and, if applicable, has entered into an agreement with the Health Plan.

Routine Electronic Transmissions are described in Article XI (“Routine Disclosures for Health Plan Transactions”) and are set forth on Exhibit C (“Routine Disclosures to Business Associates”). This list may be amended by the Privacy Official from time to time.

Whenever possible, consistent with Dow’s electronic security policy, an Electronic Transmission of PHI will meet the following criteria:

- When using open networks (*i.e.*, the internet or dial-in lines), the PHI will be encrypted before sending in order to avoid interception by parties other than the intended recipient; or
- For non-open networks, either access control (password protection) or encryption will be used to prevent parties other than the intended recipient from intercepting messages.

## **D. Security of Specific Materials and Communications**

### 1. Printed/Written Material

#### a) Generally

Responsible Persons and Business Associates must store printed or written materials containing PHI in designated secure locations when not in use. If a Responsible Person or Business Associate reasonably needs to retain the PHI other than in its designated location for a limited period, such PHI should be stored in a locked filing cabinet, desk drawer or room to which only Responsible Persons who may be called upon to access the information in accordance with this Privacy Policy have physical and administrative access.

When printed materials are in use, the Responsible Person or Business Associate must take reasonable steps to ensure that such materials are viewable only by the Responsible Person or Business Associate. For example, if the Responsible Person or Business Associate has PHI in printed material on his or her desk, he or she should put away the material before leaving his or her desk for any significant amount of time. If another person enters his or her office or cubicle while the Responsible Person or Business Associate is viewing PHI, the Responsible Person or Business Associate should remove the PHI from the view of the other person (other than another Responsible Person or Business Associate).

Under no circumstances may printed material containing PHI be removed from the Responsible Person's work site without the written approval of a Level I Responsible Person or higher. Printed or written material containing PHI that is (1) created or received by a Responsible Person and (2) is not part of a Designated Record Set or otherwise necessary or intended to be part of the Individual's file, such as personal notes not required to be retained, will be shredded prior to disposal or placed in a locked disposal receptacle and destroyed.

b) Mail

Mail addressed to a Health Plan (or known to relate to a Health Plan) and sent to Dow must be delivered to a Responsible Person. Any other correspondence addressed to Dow that contains PHI must be forwarded to a Responsible Person. Mail likely to contain PHI sent to a Business Associate shall be handled and processed in accordance with the guidelines established by the Business Associate to reasonably assure compliance with the Privacy Rules. Mail containing PHI should be handled and stored in accordance with the general guidelines for printed materials discussed under subsection (a), above. The Responsible Person or Business Associate must take reasonable steps to verify that the intended recipient of the mail is a person to whom the Responsible Person or Business Associate is required, permitted, or authorized to disclose PHI as described in this Privacy Policy. Thus, the Responsible Person or Business Associate may not routinely copy on outgoing correspondence containing PHI other persons to whom the Individual directed his or her correspondence (whether as "cc" or directly). Instead, the Responsible Person or Business Associate first must consider whether the persons the Individual copied are authorized to receive the PHI, keeping in mind that by merely directing correspondence to such persons, the Individual did not give Authorization for the Responsible Person or Business Associate to disclose PHI to them.

The Responsible Person or Business Associate mailing material containing PHI must ensure that no PHI is visible from the outside of the envelope. Unsealed mail should be handled only by the Responsible Person or Business Associate whose job involves such handling.

Outgoing mail should be addressed to the Individual at his or her address of record with the Health Plan, unless the Responsible Person or Business Associate is directed to address mail to an alternate address. Outgoing mail to a Responsible Employer or Business Associate should be sent to the Responsible Person's or Business Associate's business address. Outgoing correspondence containing PHI mailed to a Health Care Provider, non-Dow health plan, or other third party should be sent to the address provided by the requestor. The Health Plans assume that only the person(s) to whom mail is addressed will receive and open the correspondence.

c) Faxes and Print Jobs

A Responsible Person or Business Associate must take reasonable steps to ensure that all incoming faxes and print jobs containing PHI are retrieved and viewed only by a Responsible Person or Business Associate. A Responsible Person or Business Associate who transmits a fax containing PHI must take reasonable steps to verify that the intended recipient is a person to whom the Responsible Person or Business Associate is required, permitted, or authorized to disclose PHI as described in this Privacy Policy. PHI should be faxed to an Individual only upon the Individual's express request. PHI may be faxed only to a Responsible Person's or Business Associate's business fax number. Faxes to a Health Care Provider, non-Dow health plan, or other third party should be sent to the number provided by the requestor.

A Responsible Person or Business Associate must advise third parties to send faxes to a secured fax machine accessible to the Responsible Person or Business Associate. If a Responsible Person or Business Associate knows that a fax containing PHI is being sent to him or her, then the Responsible Person or Business Associate must timely retrieve the fax and safeguard the document.

A Responsible Person or Business Associate must send print jobs containing PHI to a printer accessible to the Responsible Person or Business Associate. If a Responsible Person or Business Associate prints a document containing PHI, then he or she must timely retrieve it and safeguard the document.

## 2. Electronic Information

### a) Generally

A Responsible Person or Business Associate must store computer disks and other physical storage media containing PHI in designated secure locations when not in use. See Article V.B.2. If a Responsible Person or Business Associate needs to retain the PHI other than in its designated location for a limited period, such employee must take reasonable steps to ensure that only he or she has access. For example, computer disks containing PHI should be stored in locked filing cabinets, desk drawers, rooms, or areas to which only Responsible Persons who may be called upon to access the information in accordance with this Privacy Policy have physical and administrative access. A Responsible Person or Business Associate must take reasonable steps to ensure that PHI displayed on his or her monitor is viewable only by the Responsible Person or Business Associate. For example, if the Responsible Person or Business Associate has PHI displayed on her computer screen, he should close the window containing the PHI and secure the computer before leaving his or her desk for any material amount of time.

### b) E-Mail

A Responsible Person or Business Associate who transmits mail electronically must take reasonable steps to verify that each intended recipient is a person to whom the Responsible Person or Business Associate is required, permitted or authorized to disclose PHI as described in this Privacy Policy. The Responsible Person or Business Associate also must take reasonable steps to verify that the intended recipient has sole access to the addressee e-mail account. (If the e-mail address is a Dow address, the Responsible Person or Business Associate may assume that the recipient has sole access.) Thus, the Responsible Person or Business Associate may not routinely copy on outgoing e-mail that includes PHI those persons to whom the Individual directed his or her e-mail (whether as "cc" or directly). The Responsible Person or Business Associate first must consider whether such persons are authorized to receive the PHI, keeping in mind that by merely directing correspondence to such persons, the Individual has not given his or her Authorization for the Responsible Person to disclose PHI to such persons.

E-mail to an Individual should be sent to the e-mail account on record with the Health Plan or to the e-mail address specifically provided by the Individual. E-mail to a Responsible Person or Business Associate must be sent to a business e-mail address. Messages to a Health Care Provider, non-Dow health plan, or other third party should be sent to an e-mail address provided by the requestor. In such cases, the Responsible Person or Business Associate must take reasonable steps to verify the identity of the recipient before sending communications via e-mail.

A Responsible Person or Business Associate must advise third parties to send e-mail containing PHI to a business e-mail account accessible only by the Responsible Person or Business Associate (and such other Responsible Persons and Business Associate employees with a legitimate need to use or access such PHI in the performance of Health Plan functions).

## 3. Telephonic and Other Verbal Communication

a) Generally

Before engaging in a conversation in which the Responsible Person or Business Associate may disclose PHI, a Responsible Person or Business Associate must take reasonable steps to verify that the other party (or parties) is a person to whom the Responsible Person or Business Associate is required, permitted, or authorized to disclose PHI, as described in this Privacy Policy.

b) Recordings

A Responsible Person or Business Associate who leaves a recorded message containing PHI must take reasonable steps to verify that each intended recipient is a person to whom the Responsible Person or Business Associate is required, permitted or authorized to disclose PHI, as described in this Privacy Policy; and that the intended recipient has sole access to the answering machine. A Responsible Person or Business Associate may leave a recorded message containing PHI for another Responsible Person or Business Associate at the Responsible Person or Business Associate's business phone number. A Responsible Person or Business Associate may leave a voice-mail message containing an Individual's PHI on an Individual's home answering machine only if (a) the answering machine message indicates that it is the answering machine for the Individual (or his or her residence), and (b) the Individual has instructed the Responsible Person or Business Associate to leave the message. If the Individual is a Dow employee, the Responsible Person or Business Associate may leave a message with PHI in the Individual's Dow-provided voice-mail box, unless the Individual directs otherwise.

A Responsible Person or Business Associate must advise third parties to leave recorded voice messages containing PHI at a business number accessible only to the Responsible Person or Business Associate (and such other Responsible Persons and Business Associate employees with a legitimate need to use or access such PHI in the performance of Health Plan functions.).

## **VI. Permitted Health Plan Uses and Disclosures of Protected Health Information**

A Responsible Person or Business Associate is permitted to access, request, receive, use, disclose and/or transmit PHI (i.e., engage in a Transaction) only for one of the following purposes, and subject to the restrictions described below, or in accordance with the Individual's Authorization, as described in Article VII.

### **A. Uses and Disclosures for a Health Plan's Own Payment, Treatment, or Health Care Operations**

A Responsible Person or Business Associate may engage in a Transaction involving PHI in furtherance of a Health Plan's Treatment (if any), Payment or Health Care Operations functions, provided that the following conditions are met:

- The Responsible Person or Business Associate has determined that the Transaction is for the Health Plan's own Treatment purposes, or
- The Responsible Person or Business Associate has determined that the Transaction is for the Health Plan's own Payment or Health Care Operations purposes and involves no more than the Minimum Necessary amount of PHI to accomplish the particular purpose for which the Transaction is made.

The Responsible Person or Business Associate who engages in a Transaction involving PHI is responsible for confirming that the Transaction is for Payment or Health Care Operations purposes and involves no more than the Minimum Necessary amount of PHI, except that a Responsible Person may assume that the following Transactions meet these requirements:

- A routine Transaction listed in Article XI ("Routine Disclosures for Health Plan Transactions") or Exhibit C ("Routine Disclosures to Business Associates");
- A routine disclosure to a Business Associate; and
- A Transaction engaged in under the direction and supervision of an appropriate Responsible Person at Level I or above.

Nonetheless, if the Responsible Person has reason to believe that, under the particular circumstances, the Transaction does not meet the conditions above (i.e., more than the Minimum Necessary PHI is being used), he or she must take action in accordance with Article IV.F.

Uses and disclosures for a Health Plan's own Treatment (if any), Payment or Health Care Operations purposes do not need to be documented for purposes of providing an Individual with an accounting under Article VIII.F.

### **B. Disclosures to Individuals**

A Responsible Person or Business Associate may disclose PHI directly to the Individual who is the subject of the PHI, or to his or her Personal Representative, at the request of such

Individual or Personal Representative. Such request may be made in writing or by electronic or verbal request to a Responsible Person. The Responsible Person or Business Associate who discloses PHI to an Individual must take reasonable steps to verify that the person making the request for PHI, and the recipient of such PHI, is the Individual or his or her Personal Representative. In making such a disclosure, the Responsible Person or Business Associate will comply with the safeguards on transmission of PHI set forth in Article V. Uses and disclosures under these circumstances do not need to be documented for purposes of providing the Individual with an accounting under Article VIII.F.

A Responsible Person must disclose PHI at the request of an Individual under the preceding paragraph if such information is included in the Designated Record Set. However, information subject to the attorney-client privilege, or otherwise compiled in reasonable anticipation of or use in legal proceedings, will not be disclosed.

A Responsible Person may not disclose PHI of an Individual's spouse or emancipated child at the request of the Individual under this Policy Section, unless such disclosure is authorized under a different provision of this Privacy Policy - e.g., because the Individual is the Personal Representative, the disclosure is authorized pursuant to the Individual's Authorization, as described under Article VII, or the disclosure is otherwise appropriate for Payment or Health Care Operations.

If an Individual directs a request for disclosure of PHI to a Responsible Person or Business Associate whose job function does not include making such a disclosure, the Responsible Person or Business Associate will forward the request, or refer the Individual, to an appropriate Responsible Person or Business Associate. For requests for disclosures of PHI to a third person, see the Authorization requirements under Article VII.

### **C. Disclosures to Friends and Family Members**

#### **1. General Rule**

A Responsible Person or Business Associate may not disclose an Individual's PHI to a family member, friend or other person, unless such disclosure is authorized under a specific provision of this Privacy Policy - e.g., because the Individual is a Personal Representative, the disclosure is authorized pursuant to the Individual's Authorization as described under Article VII, or the disclosure is otherwise appropriate for Payment or Health Care Operations. However, under limited circumstances a Responsible Person or Business Associate may disclose PHI to a family member, close personal friend, or other person identified by the Individual without Authorization, provided that (a) such disclosure is limited to the Minimum Necessary PHI that is directly relevant to that person's involvement with the Individual's care or payment for health care, and (b) at least one of the following conditions also is met --

1. The Individual agrees to the disclosure;
2. the Individual had an opportunity to agree or object to the disclosure and did not object;

3. based on professional judgment and the circumstances, it can reasonably be inferred that the Individual did not object to the disclosure; or
4. if the Individual was not available to agree or object, or cannot agree or object due to the Individual's incapacity (*e.g.*, due to an emergency situation verified by a hospital), but the disclosure is in the Individual's best interest.

Opportunity to object, for these purposes, means the Individual was present or otherwise available prior to the disclosure and had the capacity to make health care decisions (*e.g.*, the Individual is a party to the telephone call or meeting at which the PHI is discussed and has invited the family member or friend to participate). Uses and disclosures under these circumstances do not need to be documented for purposes of providing the Individual with an accounting under Article VIII F.

## 2. Minor Individuals

A Responsible Person or Business Associate may disclose the PHI of an unemancipated minor Individual to such Individual's parent or guardian, even if the parent or guardian is not the Individual's Personal Representative for reasons described in Article VIII.H.2, if and to the extent permitted or required under applicable state law. Uses and disclosures under these circumstances do not need to be documented for purposes of providing the Individual with an accounting under Article VIII F.

## 3. Emergencies or Disaster Relief Situations

The Health Plan also may use or disclose PHI to notify or assist in the notification of a family member, Personal Representative, close friend, another person responsible for the Individual's care, or a disaster relief organization of the Individual's location, condition, or death. Uses and disclosures under these circumstances do not need to be documented for purposes of providing the Individual with an accounting under Article VIII F.

### **D. Disclosures to a Health Care Provider for Treatment Purposes.**

A Responsible Person or a Business Associate may disclose PHI for treatment activities of a health care provider, only if the following condition is met:

- The Responsible Person or Business Associate has determined that the Transaction is for a health care provider's treatment purposes.

The disclosure for treatment purposes is not subject to the Minimum Necessary requirement.

### **E. Disclosures to a Dow Health Plan**

A Responsible Person or Business Associate may disclose an Individual's PHI to another Dow Health Plan (*i.e.*, another Responsible Person or Business Associate with respect to that plan) as long as the disclosure is for Payment or Health Care Operation purposes of either the

disclosing or recipient Health Plan, and only the Minimum Necessary amount of PHI is disclosed. If possible, De-Identified Information should be used or disclosed instead of PHI. If the disclosure is for the recipient Health Plan's use for reasons other than Payment or Health Care Operations, an Authorization first must be obtained from the Individual.

Disclosure of PHI to another Health Plan may be necessary to accomplish one of the following purposes, among others:

- Various Payment determinations, including determinations of eligibility or coverage and processing of health benefit claims - for example, information regarding claims payments under the Dow Medical Benefits Plan may be necessary for purposes of processing claims under the Dow Health Care Reimbursement Account Plan.
- Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges and utilization review activities, including pre-certification and pre-authorization of services – for example, a care determination under the Dow Medical Benefits Plan may be necessary in determining subsequent coverage of the Individual under the Dow Retiree Medical Plan.
- Conducting quality assessment and improvement activities; reduction of health care costs, case management and care coordination.
- Reviewing competence or qualifications of Health Care Providers, and evaluating provider and Health Plan performance.
- Underwriting functions.
- Conducting or arranging for fraud and abuse detection and compliance programs.
- Business planning and development, such as cost-management and planning-related analysis related to managing and operating the Health Plan.

Such disclosures must meet the Minimum Necessary requirements of Article IV with respect to both the disclosing and the receiving Health Plan. Uses and disclosures of PHI for another Health Plan's Payment or Health Care Operations purposes do not need to be documented for purposes of providing an Individual with an accounting under Article VIII F.

#### **F. Disclosures to Another Dow or UCC Benefit Plan, Other than a Health Plan**

Disclosure of PHI to a non-Health Plan may be desirable in order to process claims for disability benefits, review the competence or qualifications of Health Care Providers, or conduct fraud and abuse detection and compliance programs. A Responsible Person may disclose PHI to a non-Health Plan only if the following condition is met:

- The Responsible Person has determined that the Transaction is covered by an Authorization from the Individual whose PHI is the subject of the Transaction (or his or her Personal Representative), and that the Authorization complies with Article VII. No Authorization is necessary, however, if disclosure of PHI is made under Article VII, relating to Dow's workers compensation plan.

The Responsible Person who engages in a Transaction involving PHI under this Article is responsible for confirming that the Transaction meets the above requirements. He may assume that (a) a routine Transaction in a form approved by the appropriate Responsible Person at Level I or above, or (b) a Transaction engaged in under the direction and supervision of an appropriate Responsible Person at Level I or above, meets these requirements.

The Responsible Person or Business Associate also must document each such disclosure for purposes of providing the Individual with an accounting of disclosures as explained in Article VIII.F.

#### **G. Disclosures to the Plan Sponsor and Employer**

A Responsible Person or Business Associate may not disclose PHI to the Plan Sponsor or employer, without the Individual's Authorization except for such disclosures as provided for in the plan documents for the Health Plan. The Plan Sponsor certifies in the Health Plan documents that it agrees to the following:

- The Plan Sponsor will require the Health Plan to not use or disclose PHI other than as permitted or required by the Health Plan document or by law;
- The Plan Sponsor will ensure that any agents to whom the Plan Sponsor, through its Health Plans, provides PHI agree to be bound by the same requirements;
- The Plan Sponsor will not use or disclose PHI for employment-related decisions or in connection with any other benefit program;
- The Plan Sponsor will report to the Privacy Official any use or disclosure inconsistent with this Policy about which the Plan Sponsor becomes aware;
- The Plan Sponsor will require the Privacy Official to make available PHI in accordance with Articles VIII.B, E and F;
- The Plan Sponsor will make its Health Plans' internal practices and records related to the use and disclosure of PHI available to HHS for purposes of determining compliance with the Privacy Rule;
- If feasible, the Plan Sponsor will require the Health Plan to return or destroy all PHI and will retain no copies when no longer needed (and, if not feasible, will limit further use and disclosure to the purposes that make return or destruction infeasible); and

- The Plan Sponsor will ensure that adequate separation of the Health Plan and Plan Sponsor is established.

A Responsible Person or Business Associate may disclose PHI, in accordance with the Health Plan document, to the Plan Sponsor for Health Plan design, health care operations, and research purposes.

Such PHI includes:

- Summary Health Information for the purpose of obtaining health insurance coverage or premium bids for a Health Plan, or for making decisions to modify, amend, or terminate a Health Plan; and
- Information on whether an Individual is participating in a Health Plan, or enrollment and disenrollment information.
- PHI in Limited Data Set(s) pursuant to a data use agreement with the Plan Sponsor for research and health care operations purposes.

Uses and disclosures of PHI to the Plan Sponsor as described in this Article VI.G, do not need to be documented for purposes of providing the Individual with an accounting of disclosures under Article VIII.F.

#### **H. Disclosures to Another Covered Entity or a Health Care Provider for Payment Purposes**

A Responsible Person or a Business Associate may disclose PHI to another covered entity or a health care provider for the payment activities of the entity that receives the information, provided the following conditions are met:

- The Responsible Person or Business Associate has determined that the Transaction is for the other covered entity's or health care provider's payment purposes and involves no more than the Minimum Necessary amount of PHI to accomplish the particular purpose for which the Transaction is made, provided that the Responsible Person or Business Associate may assume disclosures of PHI pursuant to another health plan's request satisfies the Minimum Necessary requirement.

Uses and disclosures of PHI for another covered entity's or health care provider's payment purposes, as described in this Article VI.H, do not need to be documented for purposes of providing the Individual with an accounting of disclosures under Article VIII.F.

## **I. Disclosures to a Non-Dow Health Plan**

A Responsible Person or Business Associate is permitted to disclose PHI to another health plan that is a Covered Entity for that plan's payment activities, provided the following conditions are met:

- The Responsible Person or Business Associate has determined that the Transaction is for the other health plan's payment purposes and involves no more than the Minimum Necessary amount of PHI to accomplish the particular purpose for which the Transaction is made, provided that the Responsible Person or Business Associate may assume disclosures of PHI pursuant to another health plan's request satisfies the Minimum Necessary requirement

A Responsible Person or Business Associate may also disclose an Individual's PHI to another Covered Entity health plan for that plan's health care operations activities if either (1) the disclosure is for purposes of quality improvement or to review qualifications or performance of Health Care providers or health plans; or (2) the disclosure is for purposes of health care fraud and abuse detection or compliance, provided that:

- the other plan also has a relationship with the Individual;
- the Responsible Person or Business Associate has determined that the Transaction is for the other health plan's operations purposes and involves no more than the Minimum Necessary amount of PHI to accomplish the particular purpose for which the Transaction is made, provided that the Responsible Person or Business Associate may assume disclosures of PHI pursuant to another health plan's request satisfies the Minimum Necessary requirement.

Uses and disclosures of PHI for another health plan's payment or health care operations activities, as described in this Article VI.I, do not need to be documented for purposes of providing the Individual with an accounting of disclosures under Article VIII.F.

## **J. Uses and Disclosures for Health and Safety Purposes**

All uses and disclosures for health and safety purposes must first be authorized by a Level I Responsible Person. However, information subject to the attorney-client privilege or otherwise compiled in reasonable anticipation of or for use in legal proceedings will not be disclosed without prior approval of legal counsel.

A Transaction under this Article should be made only by a Responsible Person or Business Associate whose assigned job functions or contracted duties include such Transaction, or under the direct supervision of such a Responsible Person or Business Associate. Uses and disclosures under this Article must be documented for purposes of providing the Individual with an accounting as described under Article VIII.F, except when disclosure is made to a law enforcement or correctional officer about an Individual in such officer's legal custody. In all cases, only the Minimum Necessary PHI will be used or disclosed to accomplish the specific legal or law enforcement purposes.

1. Threat to Public Health or Safety.

A Responsible Person or Business Associate may use or disclose PHI as believed necessary to prevent or lessen a serious, imminent threat to public health or safety if made to someone who can prevent or lessen the threat. A Responsible Person must not, however, use or disclose PHI if the information was learned through a request by the Individual to initiate or be referred for treatment, counseling, or therapy to address the Individual's propensity to commit a crime.

2. Abuse, Neglect, or Domestic Violence.

If an Individual is a victim of abuse, neglect, or domestic violence, a Responsible Person or Business Associate may disclose the Individual's PHI to a government authority authorized by law to receive such reports. Except instances of child abuse or neglect, such disclosure must meet at least one of the following conditions:

- a) disclosure is made only to the extent required by a law;
- b) the Individual agrees to the disclosure; or
- c) the disclosure is authorized by a law or regulation and either (i) the disclosure is necessary to prevent serious harm to the Individual or others or (ii) the Individual is unable to agree to the disclosure because he or she is incapacitated but, according to an official authorized to receive the disclosure, it is necessary for immediate enforcement activity and it will not be used against the Individual.

In instances of abuse, neglect, or domestic violence not involving a child, the Responsible Person or Business Associate must inform the Individual of the disclosure unless (i) doing so would put the Individual at risk of serious harm, or (ii) the Responsible Person or Business Associate would be informing the Individual's Personal Representative and the Personal Representative is believed to be responsible for the abuse, neglect, or other injury.

If the abuse, neglect, or domestic violence does involve a child, none of the conditions (a), (b), or (c) above needs to be met. Also in such instances, the Responsible Person or Business Associate need not inform the Individual of the disclosure.

3. Public Health Activities.

A Responsible Person or Business Associate may use or disclose PHI (a) to a public health authority authorized by law to collect or receive such information for prevention purposes (e.g., disease, injury, or disability), (b) to a public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect, or (c) to a person subject to jurisdiction of the Food and Drug Administration under limited circumstances (i.e., to track product defects or improper labeling). A Responsible Person or Business Associate may also disclose information to the Plan Sponsor to evaluate whether the individual has a work-related illness or injury.

4. Health Oversight Activities.

A Responsible Person or Business Associate may use or disclose PHI to a health oversight agency for oversight activities authorized by law. Health oversight activities do not include investigations or other activities in which the Individual is the subject of that investigation or activity unless it arises out of and is related to the receipt of health care, a claim for public health benefits, or eligibility for or receipt of public benefits or services when the Individual's health is integral to the claim for public benefits or services.

**K. Uses and Disclosures Pursuant to Legal Proceedings and Law Enforcement**

The following uses and disclosures for legal and law enforcement purposes are permitted under this Privacy Policy, subject to the following conditions. Each such use or disclosure must be approved by the appropriate Level I Responsible Person. However, information subject to the attorney-client privilege or otherwise compiled in reasonable anticipation of or for use in a legal proceeding will not be disclosed without prior approval of legal counsel.

Uses and disclosures under this Section must be documented for purposes of providing the Individual with an accounting as described under Article VIII.F except when disclosure is made to a law enforcement or correctional officer for an Individual in such officer's legal custody. In all cases, only the Minimum Necessary PHI will be used or disclosed to accomplish the specific legal or law enforcement purposes.

1. Legal Proceedings with Court Order.

A Responsible Person or Business Associate will, to the extent ordered, disclose PHI in the course of a judicial or administrative proceeding in response to an order from a court or an administrative tribunal that applies to the Health Plan.

2. Legal Proceedings without Court Order.

Absent a court order, a Responsible Person or Business Associate may disclose PHI in response to a subpoena, discovery request, or other legal process that applies to the Health Plan provided one of the following conditions is met:

- a) the Responsible Person or Business Associate receives documentary evidence that (i) the requesting party provided or made a reasonable attempt to provide written notice to the Individual (including sufficient information to enable the Individual to raise an objection), (ii) the time for raising an objection has elapsed, and (iii) either no objection was raised or all objections have been resolved in a way that permits the disclosure; or
- b) the Responsible Person or Business Associate receives documentary evidence from counsel that the requesting party obtained or made a reasonable attempt to obtain a Qualified Protective Order (i.e., an agreed Qualified Protective Order has been presented to the court or the requesting party has sought such an order from the court or tribunal); or

- c) the Responsible Person or Business Associate makes reasonable efforts to notify the Individual (as described in (a) above) or to obtain a Qualified Protective Order (as described in (b) above).

3. Law Enforcement.

A Responsible Person or Business Associate may disclose PHI to a law enforcement officer for law enforcement purposes, provided the following conditions are met, if applicable:

- a) Court Orders. The disclosure is required by law or is in compliance with a court order (including court-ordered warrant, subpoena, or summons), a grand jury subpoena, or an administrative request, provided the information requested is relevant and material to a legitimate law enforcement inquiry and is limited to the purpose of that inquiry. Where reasonably possible, De-Identified Information must be substituted for the PHI.
- b) Suspects, Missing Persons, etc. The disclosure is in response to a law enforcement officer's request, and is for the purpose of locating a suspect, fugitive, material witness, or missing person and the disclosure is limited to following information:
- name and address,
  - date and place of birth,
  - social security number,
  - ABO blood type and rh factor,
  - type of injury,
  - date and time of treatment,
  - date and time of death, and
  - distinguishing physical characteristics.
- c) Crime Victims. The disclosure is in response to a law enforcement officer's request for information about an Individual who is a suspected crime victim and the Individual/victim agrees to the disclosure. If the Individual/victim is unable to agree to the disclosure because of incapacity or emergency circumstances, the Responsible Person or Business Associate will make the disclosure only if the law enforcement official represents that (i) the disclosure is necessary to determine if someone other than the Individual/victim committed a crime (ii) it is necessary for immediate enforcement activity, and (iii) it will not be used against the

Individual/victim, and (iv) the disclosure is in the Individual's/victim's best interests.

- d) Crime Related to Individual's Death. The disclosure is made to a law enforcement officer and is about a deceased Individual whose death may have resulted from a crime.
  - e) Crime on Premises. The disclosure is made to a law enforcement officer and is evidence of a crime that occurred on the Dow's premises.
4. Fugitives, Violent Crime.

A Responsible Person or Business Associate may use or disclose PHI for law enforcement identification or apprehension of an Individual because the Individual admitted participating in a violent crime that may have caused serious physical harm to the victim or where it appears that the Individual is a fugitive of lawful custody. If the Individual's admission was made in connection with a request for treatment referral, however, the Responsible Person or Business Associate is not permitted to make the disclosure without the Individual's Authorization. The disclosure must be limited to:

- the Individual's admission statement,
- name and address,
- date and place of birth,
- social security number,
- ABO blood type and rh factor,
- type of injury,
- date and time of treatment,
- date and time of death, and
- distinguishing physical characteristics.

#### **L. Uses and Disclosures Concerning Decedents**

The following uses and disclosures concerning decedents are permitted under this Privacy Policy, subject to the following conditions. Each such use or disclosure must be approved by the appropriate Level I Responsible Person. However, information subject to the attorney-client privilege, or otherwise compiled in reasonable anticipation of or for use in legal proceedings, will not be disclosed without prior approval of legal counsel.

Uses and disclosures under this Section must be documented for purposes of providing the Individual with an accounting as described in Policy Article VIII.F.

1. Post-mortem Identification, etc.

A Responsible Person or Business Associate may disclose PHI to (a) a coroner or medical examiner for purposes of identifying the decedent, determining cause of death, or other lawful purpose or (b) a funeral director as necessary for purposes of carrying out his duties. (If the requested disclosure is to a law enforcement officer and is about a deceased Individual whose death may have resulted from a crime, see Article VI.K, above.)

2. Tissue Donation.

A Responsible Person may use or disclose PHI for purposes of cadaveric organ, eye, or tissue donation to organizations engaged in procuring, banking, or transplanting such cadaveric organs, eyes, or tissues.

**M. Uses and Disclosures for Other Government Purposes**

The following uses and disclosures for governmental purposes are permitted under this Privacy Policy, subject to the following conditions. Each such use or disclosure must be approved by the appropriate Level I Responsible Person. However, information subject to the attorney-client privilege, or otherwise compiled in reasonable anticipation of or for use in legal proceedings, will not be disclosed without prior approval of legal counsel.

Uses and disclosures under this Section must be documented for purposes of providing the Individual with an accounting unless made for national security reasons or made to a correctional officer about an Individual in such officer's legal custody.

1. Armed Forces.

A Responsible Person or Business Associate may use or disclose PHI about Individuals who are members of the Armed Forces for activities necessary to assure proper execution of a military mission, provided the appropriate military authority has published a notice in the Federal Register that includes appropriate military command authorities and permitted purposes for the use or disclosure, or to a foreign military authority regarding Individuals who are foreign military personnel for the same purpose.

2. National Security.

A Responsible Person or Business Associate may use or disclose PHI to an authorized federal officer for intelligence, counter-intelligence, or other national security activities authorized by the National Security Act.

3. Federal Protective Services.

A Responsible Person or Business Associate may use or disclose PHI to an authorized federal officer for the provision of protective services to the President, foreign heads of state or other designated persons, or for the conduct of investigations authorized by law.

4. Correctional Institution or Lawful Custody.

A Responsible Person or Business Associate will use or disclose PHI to a correctional institution or law enforcement officer who has lawful custody of the Individual if the information is necessary for provision of health care to the Individual or for ensuring the Individual's, other inmates', or correctional institution employees' health or safety.

**N. Disclosures to U.S. Department of Health and Human Services**

A Responsible Person or Business Associate may disclose PHI to the Secretary of Health and Human Services when requested by the U.S. Department of Health and Human Services for purposes of determining a Health Plan's compliance with the Privacy Rule. Each such use or disclosure must be approved by the appropriate Level I Responsible Person. However, information subject to the attorney-client privilege, or otherwise compiled in reasonable anticipation of or for use in legal proceedings, will not be disclosed without prior approval of legal counsel.

Uses and disclosures under this Section must be documented for purposes of providing the Individual with an accounting of disclosures as described under Article VIII.F.

1. Health Oversight Activities

A Responsible Person will use or disclose PHI to a health oversight agency for activities authorized by law. Health oversight activities do not include investigations or other activities in which the Individual is the subject of that investigation or activity unless it arises out of and is related to the receipt of health care, a claim for public health benefits, or eligibility for or receipt of public benefits or services related to a patient's health.

## **VII. Uses and Disclosures Only With Authorization**

### **A. Authorization Required**

Generally, a Health Plan will not use or disclose PHI for reasons other than Payment, Health Care Operations, and - less frequently - the other purposes described under Article VI. For all other uses and disclosures, a Health Plan must obtain the Individual's Authorization prior to the use and disclosure and each such use or disclosure must be consistent with the Authorization given for that use or disclosure. A Health Plan will request an Authorization only if there is a need to disclose PHI for reasons other than Payment, Health Care Operations, or reasons not otherwise permitted in Article VI.

Authorizations must be obtained and tracked by the Health Plan. If the Authorization is requested by the Health Plan, the Individual must be provided with a copy of the Authorization.

### **B. Required Elements for a Valid Authorization**

An Authorization is not valid unless it is written in plain language and it contains all of the following elements:

1. a description of the PHI to be used or disclosed;
2. the name or job titles of the person(s) authorized to make the use or disclosure described;
3. the name or job titles of the person(s) to whom the disclosure may be made;
4. an expiration date or expiration event related to the Individual or to the purpose of the use or disclosure;
5. a description of each purpose of the requested use or disclosure or if the Authorization is made at the request of the Individual, or statement to that effect;
6. a statement of the Individual's right to revoke (including any restrictions on the right to revoke the Authorization) and a description of the procedure for the Individual to revoke the Authorization;
7. a statement that the PHI might be further disclosed by the recipient and might not thereafter be protected by the Privacy Rule; and
8. the Individual's signature and the date of signature, or that of his Personal Representative together with a description of that Personal Representative's authority to act on behalf of the Individual.

### **C. Authorization as a Condition of Enrollment**

An Authorization to obtain PHI from another Covered Entity may be required as a condition for enrollment in a Health Plan for purposes of determining eligibility for benefits

under a Health Plan prior to the Individual's enrollment in the Health Plan, or if the PHI is needed for the Health Plan's underwriting or risk rating determinations. A copy of the signed Authorization must be given to the Individual.

**D. Revocation of an Authorization**

An individual may revoke an Authorization in writing at any time except to the extent that the Health Plan already has acted in reliance on the Authorization or, if the Authorization was a condition for enrollment under an insurance contract, where the insurer has the legal right to contest a claim or the insurance policy, itself. The Individual must deliver the written revocation to the Privacy Official who will notify the relevant Responsible Person(s).

**E. Recordkeeping**

The Privacy Official must retain the Authorization and any related revocations for at least six years from the later of (a) the effective date or (b) expiration date.

## **VIII. Individuals' Rights Regarding Protected Health Information**

An Individual has a number of rights under the Privacy Rule, including the right to a privacy Notice containing a Health Plan's legal duties regarding uses and disclosures of PHI, the right to access and amend PHI in the Designated Record Set, the right to request restrictions on uses and disclosures of PHI, and the right to an accounting of certain uses and disclosures of PHI. Under no circumstances will Health Plan enrollment or benefit payment be conditioned on an Individual's waiver of his rights under the Privacy Rule.

The Health Plan or Plan Sponsor may contract with a Business Associate(s) to fulfill the responsibilities described in this Article VIII, Sections B, C, D, E, F, G, and H. For these Health Plans, the applicable Business Associate's privacy policy with respect to these matters will apply in lieu of this Article VIII.

In the cases of the insured Health Plans, the insurance carriers and HMOs or DMO's will fulfill the responsibilities of the Privacy Rule on behalf of these Health Plans, including the requirements of Article VIII of this Privacy Policy. In most situations, the insurance carrier's or the HMO's or DMO's privacy policy will apply in lieu of the Dow or UCC Health Plan's privacy policy.

### **A. Privacy Notice**

The Plan Sponsor, on behalf of its Health Plans, must notify Individuals of the Health Plans' uses and disclosures of PHI and the Health Plans' legal duties with respect to PHI. The terms of the Notice also bind all Business Associates, to the extent the Business Associates use or disclose PHI on behalf of a Health Plan. Such Notice must be provided to each Individual at the time of enrollment for the first time in the Health Plan and must be posted on the Dow IntraNet. Each covered dependent of a Covered Participant will be deemed to have received a copy of the Notice if the Notice is provided to the Covered Participant. The Notice must be revised whenever there is a material change to the uses and disclosures, Individuals' rights, the Health Plans' duties, or other privacy practices stated in the Notice. Revised Notices must be distributed to Individuals and posted on the Dow website for employees within 60 days of the material change. The Privacy Official must maintain a copy of each version of the Notice for a period of at least six years from the date last effective.

Once every three years, the Health Plans must notify Individuals of their right to obtain a copy of the Notice and how to do so. Mailing of the Notice with the Choices enrollment materials by first class mail to the last known address is deemed sufficient to fulfill the distribution to Individuals requirement. If the Individual agrees, and the Health Plans makes this option available, the Notice may be delivered electronically. If the Health Plans become aware that electronic delivery has failed, a paper copy must be provided. All Individuals have the right to request a paper copy of the Notice by mailing a request to the Privacy Official.

### **B. Access to Protected Health Information**

Except as otherwise provided in this Section B, the Health Plan will permit an Individual to inspect and obtain a copy of his or her PHI within a Designated Record Set. A request for access must be made in writing and submitted to the Privacy Official.

If the Health Plans charge a fee to copy and/or mail the requested PHI, the Individual will be notified of the fee in advance.

1. Timing of Response and Providing Access.

Within 30 days of receiving the request (or 60 days if the requested PHI is not maintained or accessible on-site), the Privacy Official must provide the requested access, provide a written denial notice, or provide written notice that an extension of time is needed to respond to the request. If access is to be granted but cannot be granted within 30 days (60 days) of the request, a Health Plan will have up to 30 additional days to provide access as long as the Individual is notified in writing of the reason for the delay and the additional time needed to comply before the expiration of the first 30-day (60-day) period. If the information is maintained by a Business Associate for a Health Plan, the Privacy Official must instruct the Business Associate to provide the Privacy Official with copies of the PHI so that the requested access can be provided within these time frames.

2. Denying the Request.

A Health Plan will deny the Individual's request to inspect or obtain a copy of PHI if any of the following apply:

- a) the request is for information compiled in reasonable anticipation of, or use in, a civil, criminal, or administrative action or proceeding; and
- b) The PHI was obtained from someone other than a Health Care Provider under a promise of confidentiality and the requested access, if granted, likely would reveal the source of information.
- c) A licensed health care professional has determined that the requested access, if granted, likely would endanger the Individual or another person.
- d) The PHI makes reference to another person (other than a Health Care Provider) and a licensed health care professional has determined that the requested access, if granted, likely would cause substantial harm to that referenced person.
- e) The request is made by a Personal Representative and a licensed health care professional has determined that the requested access, if granted, likely would cause substantial harm to the Individual or another person.

If access is denied for reason (c), (d), or (e) above, the Individual has the right to have the denial reviewed by a licensed health care professional designated by the Privacy Official to act as a review officer. This review officer cannot be someone who participated in the original decision to deny access. Each denial must be provided in writing and include (i) a statement of the reason for denial, (ii) the procedure for requesting review of the denial, if applicable, and (iii) the procedure for filing a complaint with the Privacy Official (with contact information) or the U.S. Department of Health and Human Services. If requested, the review must be promptly

given and, if access is again denied on review, written notice must be given promptly to the Individual.

If the Individual requested access to PHI not maintained by or for a Health Plan, but the Privacy Official knows where the information is maintained, the Privacy Official must inform the Individual where to direct his request.

3. Record Retention.

The Health Plans must retain a record of each request for access, including: the request, responses to the request, the identity of the Responsible Person who received and processed the request for access, the specific PHI subject to the access, and any other related documentation. Such documentation must be maintained for at least six years from the date created.

**C. Request for Restriction on Uses and Disclosures**

An Individual may request that a Health Plan restrict in a specified way uses and disclosures of PHI:

- for the Health Plan's Payment and Health Care Operations;
- for another Covered Entity's treatment, payment or health care operations; or
- to family members and friends without an Authorization.

Such a request must be made in writing. Written requests must be submitted to the Privacy Official.

1. Privacy Official May Grant or Deny the Restriction.

The Privacy Official may grant or deny the restriction at his sole discretion. The Privacy Official will notify the requester of his decision in writing.

2. Effect of Restriction.

If a Health Plan agrees to the requested restriction, Responsible Persons and Business Associates will not thereafter use or disclose PHI inconsistently with the restriction unless the restriction agreement is terminated or any such inconsistent use or disclosure is necessary to provide emergency treatment. If the Responsible Person or Business Associate discloses the restricted PHI to a Health Care Provider in such emergency, the Responsible Person or Business Associate must request that the provider not further disclose it. This restriction will not apply to uses and disclosures conducted prior to a Health Plan's agreement to the restriction.

The Health Plan may terminate a restriction agreement by informing the Individual of such termination in writing. The termination of the restriction will be effective only with respect to PHI created or received after the Health Plan has so informed the Individual, unless the Individual agrees to the termination orally or in writing, and such agreement is documented and submitted to the Privacy Official.

3. Standard for Restrictions.

Because it is the Health Plans' policy not to use or disclose PHI other than as minimally necessary to perform Payment or Health Care Operations or for other limited purposes discussed in Article VI above, the Privacy Official does not expect to grant requests for additional restrictions on the use or disclosure of PHI. When such additional restriction is important for the safety or well-being of the Individual, however, and the requested restriction can be granted without imposing an undue burden on the Health Plans, the Privacy Official will endeavor to grant the request.

4. Record Retention.

The Health Plans must retain a record of each restriction request, including: the request, responses to the request, agreements, termination-of-agreement notices, the identity of the Responsible Person who received and processed the request, and other related documents for at least six years from the date created or last effective, whichever is later.

**D. Request for Alternate Address/Confidential Communication**

An Individual may request that the Health Plans communicate his PHI by alternate means or at alternative locations. The Health Plans will consider requests that can be granted without imposing an undue burden on the Health Plans or its Business Associates. However, the Health Plans must accommodate each reasonable request that does not impose an unreasonable burden on the Health Plans or its Business Associates if the Individual clearly states that the disclosure of the PHI by the standard means or at the regular location could endanger him. Such a request must be made in writing, include the alternative communication means or alternate location, and if applicable, include a statement that, if such disclosure request is not granted, it could endanger the Individual. Such request must be submitted to the Privacy Official.

The Health Plans must retain a record of each request for confidential communication including: the request, responses to the request, the identity of the Responsible Person who received and processed the request, and other related documents for at least six years from the date created or last effective, whichever is later.

**E. Amendment of Protected Health Information**

An Individual has a right to request that a Health Plan amend his PHI within a Designated Record Set. Such a request must be made in writing and submitted to the Privacy Official. The request for amendment should include the reasons for and any evidence to support the need for amendment.

1. Timing of Response.

Within 60 days of receiving the request, the Privacy Official must either amend the information as requested, provide a written denial notice, or provide written notice that an extension of time is needed to respond to the request. If a determination cannot be made within 60 days of the request, then the Health Plan can extend the time limit by up to an 30 additional

days, as long as the Individual is notified in writing of the reason for the delay and the additional time needed to comply before the expiration of the first 60-day period.

2. Granting the Request.

If the request is granted, the Privacy Official must (a) amend the information, (b) notify Business Associates who may already have relied or may rely in the future on such information, (c) inform the Individual of the amendment, and (d) with the Individual's agreement, notify persons identified by the Individual as needing notice of the amendment.

3. Denying the Request.

The Individual's request to amend his PHI will be denied if the Privacy Official determines that –

- a) the information was not created by a Health Plan (unless the creator no longer is available to amend it and the Privacy Official otherwise determines that it should be amended under this Policy);
- b) it is not part of the Designated Record Set;
- c) it is not accessible to the Individual under Article VIII.B.2; or
- d) the information is complete and accurate.

If the request is denied, the Privacy Official must provide the basis for the denial in writing. The written denial also must inform the Individual of his right to (a) submit a written statement to the Health Plan disagreeing with the denial, and the procedure for such submission or (b) if he chooses not to submit a disagreement, his right to ask that his request and the denial of such request accompany any future disclosures of the subject PHI, or (c) the procedure for filing a complaint with the Privacy Official or Secretary of Health and Human Services. The Privacy Official will rebut statements of disagreement in writing to the Individual, if rebuttal is applicable. Any such request for amendment, statement of disagreement, and rebuttal must be included with future disclosures of the subject PHI.

4. Notice of Amendment from Another Entity.

If a Health Plan receives notice of an amendment from a Health Care Provider or other Covered Entity under the Privacy Rule, the Privacy Official must amend the subject PHI if included as part of a Designated Record Set.

5. Record Retention.

The Health Plan must retain a record of each request for amendment including: the request, responses to the request, the identity of the Responsible Person who received and processed the request, and any other related documents for at least six years after the date created or last effective, whichever is later.

## **F. Accounting.**

If requested, a Health Plan will provide an accounting of certain Health Plan disclosures of PHI (including disclosures by Business Associates) within the six-year period prior to the request, or since the HIPAA Compliance Date (April 14, 2003), whichever is less. Such requests for an accounting may be made orally to the Privacy Official or in writing. Written requests must be submitted to the Privacy Official.

The accounting must be in writing and include for each disclosure, the date, name of recipient (and address, if known), description of information disclosed and purpose for the disclosure (or a copy of the request for disclosure or the Individual's Authorization).

An Individual does not have the right to an accounting of Health Plan disclosures made –

1. to carry out Treatment, Payment or Health Care Operations;
2. for another Covered Entity's treatment, payment or health care operations;
3. to the Individual about his own PHI;
4. to family members and friends;
5. pursuant to an Authorization;
6. for national security or intelligence purposes;
7. to correctional institutions or law enforcement officer;
8. to the Plan Sponsor for enrollment and disenrollment information, Summary Health Information, and Limited Data Set information; or
9. prior to April 14, 2003.

A Health Plan will provide one such accounting in a 12-month period without charge and may charge a reasonable fee for subsequent accountings requested in the same 12-month period. The Individual's right to an accounting will be subject to certain public health and law enforcement related restrictions provided under the Privacy Rule.

### 1. Timing of Response.

Within 60 days of receiving the request, the Privacy Official must either provide the Individual with an accounting or provide written notice that an extension of time is needed to respond to the request. If an extension of time is needed, the Health Plan will have up to 30 additional days to provide the accounting, as long as the Individual is notified in writing of the reason for the delay and the additional time needed to comply before the expiration of the initial 60-day period.

Upon receiving a request for an accounting, the Privacy Official will request an accounting of disclosures from the Business Associates. The Business Associates will provide

the Privacy Official with an accounting of its disclosures, if any, so that a complete accounting of Health Plan (including Business Associate) disclosures can be provided within these time frames.

## 2. Record Retention.

The Health Plans must retain a record of each request for an accounting including: the request, responses to the request, the identity of the Responsible Person who received and processed the request, the information subject to the accounting and the written accounting provided to the Individual. Such documentation must be maintained for at least six years after the date created.

### **G. Complaints**

An Individual has a right to complain to the Privacy Official and to HHS about this Privacy Policy and the Health Plans' compliance with the Privacy Rule. The Notice must inform each Individual of his right to complain to HHS and the Privacy Official and the procedure for making such complaint.

The Plan Sponsors, their employees, the Health Plans, and the Business Associates must refrain from retaliating against or intimidating the complainant in any way for complaining. The complainant and any involved employees must cooperate with the Privacy Official's or HHS's investigation and other action taken in response to the complaint. No person will be intimidated, threatened, or discriminated against in any way for participating in an investigation of a complaint.

The Privacy Official must address each complaint promptly. The Privacy Official first will investigate the complaint and document his investigation efforts and findings. To the extent that the Privacy Official finds that PHI has been used or disclosed in violation of this Privacy Policy, he or she must take immediate steps to mitigate any harm caused by the violation. The Privacy Official also must take steps to minimize the possibility that such a violation will recur. Employees found to have violated this Privacy Policy are subject to disciplinary action. If a Business Associate is found to have violated this Policy or its Business Associate contract, the Privacy Official must take actions in accordance with Article X.B.

The Privacy Official will provide a written response to the complainant if he or she submitted the complaint in writing (other than anonymously). The response will include a description of the investigation and findings and, to the extent appropriate, a description of the actions taken to mitigate harm and prevent recurrence.

The Privacy Official must retain documentation describing the complaint (or, if submitted in writing, a copy of the complaint), investigation, findings, mitigation and prevention steps, and response (or a copy of the response). Such documentation must be maintained for a period of at least six years from the date created or last effective, whichever is later.

## H. Personal Representatives

### 1. Rights of Personal Representatives

An Individual's Personal Representative has the authority to exercise the rights and responsibilities described in this Article on behalf of the Individual regarding PHI relevant to that person's representation of the Individual.

Responsible Persons and Business Associates must take reasonable steps to confirm the status of persons purporting to be Personal Representatives. For example, guardians and conservators will be required to produce documents verifying such appointments.

### 2. Circumstances Under Which a Personal Representative is Not Treated as Such

The parent(s) or guardian of an unemancipated minor Individual will not be treated as the minor Individual's Personal Representative:

- to the extent the minor Individual has the legal right to consent to health care without anyone else's consent, if the minor (a) has consented to such health care, and (b) has not requested that such parent or guardian be treated as his Personal Representative with regard to that health care; or
- the parent or guardian has consented to confidentiality between the Individual and the Individual's health care provider.

If an appropriate Level I Responsible Person, or a Business Associate employee designated by the Business Associate to make such determinations, believes that the Personal Representative has subjected or may subject the Individual to domestic violence, abuse, or neglect or may otherwise endanger the Individual, the Health Plans may elect not to treat such person as the Individual's Personal Representative.

Even if a person is not treated as an Individual's Personal Representative as described above, a Responsible Person may disclose PHI to the person to the extent permitted under Article VI.

## **IX. Business Associates**

### **A. Obligations of Business Associates**

The Health Plans may subcontract some or all of the Health Plans' administration to a Business Associate. Like a Health Plan, a Business Associate must safeguard PHI and enable the Health Plans to otherwise comply with the Privacy Rule with respect to PHI created or received on behalf of the Health Plans. The Privacy Official must obtain satisfactory assurance that each such Business Associate will safeguard PHI and enable compliance with the Privacy Rule. In general, satisfactory assurance will be obtained by executing a contract with the Business Associate that addresses the Business Associate Privacy Rule requirements.

## **X. Health Plan Privacy Administration**

### **A. Written Policy**

The Privacy Official is responsible for maintaining this Privacy Policy. The adoption and amendments to the Privacy Policy must be approved by the Vice President, Human Resources. The Privacy Official must ensure that material amendments are in writing and communicated to Responsible Persons, Business Associates, and other necessary parties. The Privacy Official must enforce this Privacy Policy and must take reasonable steps to ensure that all Responsible Persons adhere to this Privacy Policy. If a circumstance arises that is unforeseen by this Privacy Policy, or if a Responsible Person believes that a deviation from the Privacy Policy is necessary, the Responsible Person must consult with the Privacy Official regarding such unforeseen circumstance or deviation. The Privacy Official will decide how to apply this Privacy Policy to such unforeseen circumstance or whether to deviate in any way from the Privacy Policy.

### **B. Enforcement of Privacy Policy**

#### **1. Reporting Privacy Policy Violations**

Responsible Persons and Business Associates must report instances of a violation of the Privacy Policy to the Privacy Official immediately upon discovery. If the Privacy Official is involved in the violation in a way that makes it impractical or futile for the Responsible Person or Business Associate to report the violation to the Privacy Official, the Responsible Person or Business Associate must report the violation to the Vice President, Human Resources.

The Plan Sponsors, their employees, the Health Plans, and all Business Associates are prohibited from retaliating against or intimidating any person for reporting a Privacy Policy violation to the Privacy Official or to HHS in accordance with this Policy. A Plan Sponsor's employee who reports a Privacy Policy violation must cooperate with the investigation of the reported violation.

#### **2. Disclosures by Whistleblowers**

A Responsible Person or Business Associate may disclose PHI to a health oversight agency or public health authority charged with investigating or overseeing the conduct or conditions of the Health Plans, or to an attorney retained by a Responsible Person or Business Associate for purposes of determining the Responsible Person's or Business Associate's legal options, if the Responsible Person or Business Associate, in good faith, believes that a Health Plan has engaged in unlawful conduct. A Responsible Person will not be sanctioned or retaliated against for good-faith disclosures in accordance with this Article X.B.2.

### 3. Response to Report of Privacy Policy Violations

The Privacy Official must address each reported Privacy Policy violation promptly. The Privacy Official first will investigate the reported violation and document his investigation efforts and findings. To the extent that the Privacy Official finds that PHI has been used or disclosed in violation of the Privacy Policy, he or she must take immediate steps to mitigate any harm caused by the violation. The Privacy Official also must take steps to minimize the possibility that such a violation will recur.

Any Plan Sponsor employee found to have violated the Privacy Policy will be subject to disciplinary action. Such disciplinary action also applies to an employee who fails to mitigate harm resulting from an impermissible use or disclosure of PHI or who intimidates or retaliates against another employee for reporting a Privacy Policy violation. If a Business Associate is found to have violated this Policy or its Business Associate contract, the Privacy Official must consider the appropriate course of action consistent with the Business Associate's contract.

### 4. Recordkeeping

The Privacy Official must retain documentation describing the reported Privacy Policy violation, investigation, findings, mitigation, and prevention steps. Such documentation must be maintained for a period of at least six years from the date created or last effective, whichever is later.

## **C. Employee Training**

### 1. Employees Who Must Receive Privacy Policy Training

All Responsible Persons on the HIPAA Compliance Date will receive training on this Policy no later than the HIPAA Compliance Date. Following the HIPAA Compliance Date, new Responsible Persons must be trained regarding the Privacy Policy within a reasonable time after such employee begins working as a Responsible Person. Job titles or job categories of Responsible Persons are identified under Article III.B and Exhibit B.

Similarly, Business Associates must train their employees on this Policy, to the extent it applies to the Business Associate, and or its own policy, if any.

### 2. Description of Privacy Policy Training

The Privacy Official is responsible for developing and delivering Privacy Policy training programs for Responsible Persons. The scope and content of Privacy Policy training depends on the job duties of the Responsible Persons subject to training at any given time and the extent and purposes for which they access and use PHI for their job duties. All Responsible Persons must be trained on the minimum necessary requirements, and the principles of and specific requirements for safeguarding PHI, as well as the fact that compliance with the Privacy Policy is a requirement of their jobs. In addition, when applicable, Privacy Policy training covers

permissible uses and disclosures of PHI, Individuals' rights with respect to PHI, recordkeeping, and other administrative requirements.

The Privacy Official must ensure that additional training is provided if the Privacy Policy changes in a material way. Such additional training must be delivered within a reasonable time after the change becomes effective.

### 3. Recordkeeping

The Privacy Official must maintain a record of each instance of Privacy Policy training for a period of at least six years from the date of the training. Such record includes the names of those attending, the date when and location where training was provided, a copy of any training materials, and a description of the delivery format (*e.g.*, web-based, video, live instruction, etc.).

#### **D. Recordkeeping Activities**

The Privacy Official must retain all documentation as described throughout the Privacy Policy either in paper or electronic format for at least six years from the date of creation or effective date, whichever is later. Such recordkeeping requirements apply to:

- this Privacy Policy and all modifications thereto;
- Authorizations and revocations thereof;
- training records;
- designations of Privacy Official;
- complaints and related investigations and sanctions;
- Individuals' requests for restrictions on, access to, amendments and accountings of uses and disclosures; and
- uses and disclosures of PHI subject to an individual's right to an accounting, access or amendment.

These recordkeeping requirements are explained in greater detail in the applicable Articles of this Policy.

**XI. Routine Health Plan Transactions**

The following generally describes routine Health Plan Transactions performed by Responsible Persons. Guidelines for uses and disclosures of PHI by Business Associates will be documented by the Business Associates, as appropriate.

Routine transactions of PHI to Business Associates are described in Exhibit C.

**A. Resource Center**

Responsible Persons in the Resource Center create and receive PHI from individuals who have questions about their Health Plan benefits and from Business Associates (as permitted under this Policy). A Responsible Person in the Resource Center may use or disclose PHI as follows:

<b>DESCRIPTION OF HEALTH INFORMATION</b>	<b>REASON FOR USE/DISCLOSURE</b>	<b>MINIMUM NECESSARY PHI</b>
Disclosure of Health Plan enrollment and eligibility information	Disclosure of PHI to an Individual to direct him to the correct Health Plan administrator, HMO, or insurer	No limit - disclosure of Individual's own PHI
	Disclosure of a dependent family member's PHI to a Covered Participant to direct the Covered Participant to the correct Health Plan administrator HMO, or insurer	Name and contact information for appropriate administrator, HMO, or insurer for relevant Health Plan
	Disclosure of a minor child's PHI to a parent or guardian to direct the parent or guardian to the correct Health Plan administrator, HMO, or insurer	Name and contact information for appropriate administrator, HMO, or insurer for relevant Health Plan
	Disclosure of an Individual's own Enrollment or Eligibility information to the Individual	No limit – disclosure of Individual's own PHI
	Disclosure of a dependent's Eligibility or Enrollment information to the Covered Participant	Eligibility and Enrollment data

<b>DESCRIPTION OF HEALTH INFORMATION</b>	<b>REASON FOR USE/DISCLOSURE</b>	<b>MINIMUM NECESSARY PHI</b>
	Disclosure of a minor child's Eligibility or Enrollment information to a parent or guardian	Eligibility and Enrollment data
	Disclosures to Health Plan administrators, HMO, insurers, and Responsible Persons for Payment or Health Care Operations	Eligibility and Enrollment data
Claim-related medical information	Use of PHI obtained from an Individual or Responsible Person and disclosure to the appropriate Health Plan administrator, HMO, insurer, or Responsible Person to assist or inform the Individual about a claim or coverage issue, or status of his benefits	Varies, but must be limited to the relevant Individual(s) and only relevant Health Plan(s)
Claim-related medical information	Disclosures to Health Plan administrators, HMO, insurers, and Responsible Persons for Payment or Health Care Operations	Varies, but must be limited to the relevant Individual(s) and only relevant Health Plan(s). The relevant Individuals may include similarly situated Individuals in order to obtain consistency in claims adjudication and administrative precedent.

**B. HR Service Center and Retiree Service Center**

Responsible Persons in the HR Service Center and the Retiree Service Center create and receive PHI from individuals who have questions about their Health Plan benefits and from Business Associates (as permitted under this Policy). A Responsible Person in the HR Service Center or Retiree Service Center may use or disclose PHI as follows:

<b>DESCRIPTION OF HEALTH INFORMATION</b>	<b>REASON FOR USE/DISCLOSURE</b>	<b>MINIMUM NECESSARY PHI</b>
Disclosure of Health Plan enrollment information	Disclosure of PHI to an Individual to direct him to the correct Health Plan administrator, HMO, or insurer	No limit – disclosure of Individual’s own PHI
	Disclosure of a dependent family member’s PHI to a Covered Participant to direct the Covered Participant to the correct Health Plan administrator HMO, or insurer	Name and contact information for appropriate administrator, HMO, or insurer for relevant Health Plan
	Disclosure of a minor child’s PHI to a parent or guardian to direct the parent or guardian to the correct Health Plan administrator, HMO, or insurer	Name and contact information for appropriate administrator, HMO, or insurer for relevant Health Plan
	Disclosure of an Individual’s own enrollment information to the Individual	No limit – disclosure of Individual’s own PHI
	Disclosure of a dependent’s Eligibility or Enrollment information to the Covered Participant	Eligibility and Enrollment data
	Disclosure of a minor child’s Eligibility or Enrollment information to a parent or guardian	Eligibility and Enrollment data
Claim-related medical information	Use of PHI obtained from an Individual and disclosure to	Varies, but must be limited to the relevant

DESCRIPTION OF HEALTH INFORMATION	REASON FOR USE/DISCLOSURE	MINIMUM NECESSARY PHI
	the appropriate Health Plan administrator, HMO, insurer, or Responsible Persons, to assist the Individual with a claim or coverage issue	Individual(s) and only relevant Health Plan(s)

**C. Payroll**

A Responsible Person working in the Payroll Department may use or disclosure PHI for purposes of maintaining, processing and supporting the payroll function within Dow. The Responsible Person will use or disclose only the Minimum Necessary PHI to perform his job duties.

Copies of paychecks or electronic payroll data displaying Health Plan enrollment, coverage or dependent information will only be available to the Individual who is the subject of the PHI or a Responsible Person whose job duties involve the need to access such information.

**D. Information Systems**

A Responsible Person working in the Information Systems Department or a Business Associate supporting that Department may use or disclose PHI for purposes of designing and supporting human resources information systems (HRIS) or other benefits-related information systems or for retrieving or disclosing PHI via electronic means. The Responsible Person or Business Associate will use or disclose only the Minimum Necessary PHI to perform his job function.

**E. Internal Auditors**

A Responsible Person whose job function includes internal audits of Plan Sponsor operations may use or disclose PHI for purposes of performing internal audits for reviewing claim processing under a Health Plan, reviewing the Health Plan’s or Dow’s eligibility and enrollment data, Health Plan quality control, HIPAA compliance purposes, and other matters involving health care operations. In all cases, the Responsible Person will use only the Minimum Necessary PHI to perform his job function.

**F. Strategic Center**

Plan Sponsor employees working in the Strategic Center may not access or use PHI unless the employee is a designated Responsible Person under Exhibit B. Such employees shall not solicit PHI from an Individual or from a Responsible Person, and Responsible Persons may not disclose PHI to Strategic Center employees, managers, or other Plan Sponsor employees who are not Responsible Persons without the Individual’s Authorization. Certain employees working in the Strategic Center have a separate role from the Plan Sponsor’s role. These employees also have the role of Plan Administrator for certain Health Plans, and have been authorized to act as the final appellate claims reviewer for such Health Plans. When performing

the Plan Administrative functions, such Strategic Center employees are Responsible Persons who are performing “routine transactions”; ”, and they shall have the same authority to create, use and disclose PHI as the Resource Center when performing the Plan Administrator’s function.

#### **G. Legal**

A Responsible Person working in the Legal Department may use or disclosure PHI for purposes of responding to issues or questions regarding the Health Plans and this Policy from the Privacy Official, other Responsible Persons, and from Business Associates. The Responsible Person will use or disclose only the Minimum Necessary PHI to perform his job duties.

#### **H. Pension/Retirement Counseling**

A Responsible Person may use and disclose information about enrollment and premium amounts required for Health Plan coverage to the pension plan in order to obtain payment of the premiums from the pension plan. A Responsible Person may use and disclose eligibility, enrollment and general information about the benefits available under the Health Plan to the Individual (and the Individual’s family member if the Individual is also present).

#### **I. Records Retention Center**

A Responsible Person at the Records Retention Center may sort, store, and dispose of PHI in accordance with the Records Management Policy and this HIPAA Privacy Policy. The Responsible Person will use or disclose only the Minimum Necessary PHI to perform his job duties.

#### **J. Health Services Department**

Dow’s Health Services Department may use and disclose PHI for purposes of payment and health care operations with respect to the Dow Executive Physical Examination Program.

**K. Global Reporting Team**

The Health Plans may disclose enrollment and disenrollment information to Dow’s Global Reporting Team (a portion of the Human Resources function).

**L. Retirement Board**

The voting members of the Retirement Board consist of Responsible Persons. The Retirement Board creates and receives PHI from individuals and from other Responsible Persons who administer The Dow Chemical Company Retirement Health Care Assistance Plan (“RHCAP”). The Retirement Board may use or disclose PHI as follows:

DESCRIPTION OF HEALTH INFORMATION	REASON FOR USE/DISCLOSURE	MINIMUM NECESSARY PHI
RHCAP enrollment, eligibility, individual account and claims information	Use/Disclosure of an Individual’s own PHI to the Individual to inform him about a decision on his claim or about his RHCAP account or his RHCAP benefits	No limit - disclosure of Individual’s own PHI
	Use of PHI by Responsible Person(s) and disclosure to other Responsible Person(s) to determine eligibility, enrollment, RHCAP account status and history, and to adjudicate claims, and perform other Payment tasks.	Varies, but must be limited to the relevant Individual(s). The relevant Individuals may include similarly situated Individuals in order to obtain consistent claims adjudication and administrative precedent.

## **XII. Security of Electronic PHI**

### **A. Introduction**

This section of the Privacy Policy is intended to comply with the Security Regulations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) as it pertains to the electronic storage and transmission of ePHI (45 CFR Part 164, referred to as the “Security Regulations”). This section of the Privacy Policy may be referred to as the “HIPAA Security Policy”.

The Dow Chemical Company and Union Carbide Corporation, a subsidiary of The Dow Chemical Company, as Health Plan sponsors, maintain their commitment to safeguard and keep confidential the individual health information of their employees and their families. Consistent with the requirements of the Security Regulations, any electronic Protected Health Information (ePHI) stored or transmitted by, or on behalf of a Health Plan will be protected against anticipated threats or hazards to the security or integrity of ePHI and protected against prohibited disclosures of such information.

### **B. Integration with Other Dow Policies**

This Security section of the Privacy Policy adopts and incorporates by reference Dow’s Information Systems’ security policies, which are located at: [Policies: Information Security: MTMOIT](http://manage-info.intranet.dow.com/security/policies/is_p.asp) ([http://manage-info.intranet.dow.com/security/policies/is\\_p.asp](http://manage-info.intranet.dow.com/security/policies/is_p.asp)) These IS policies are an integral part of the Privacy Policy, in particular the HIPAA Security Policy. The IS security website, as of April 20, 2005, includes the following Information Security policies of The Dow Chemical Company, which may be updated by Dow from time to time:

- Corporate Policy on Computer Systems and Telecommunications Security
- Data Protection and Data Privacy Compliance
- Dow Information Handling Policy
- E-Mail Security Policy
- Information Security Standards – List
- Information Service Provider Policy
- Internet Security Policy
- Network Device Connectivity Policy
- Partner-Supported Applications Policy
- Password Security Policy
- Records Management Policy
- Virus Protection policy
- Wireless Data Communications Security Policy

In addition, IS has a number of other policies:

- Information Security Center Investigation Process
- Information Security Policy Enforcement Process
- I/S Methodology Workbench

Change Integration and Implementation Procedures  
Dow Cybersecurity Strategy  
Dow Policy on Protection of Personal Employee Data  
Dow Workstation DWS2003 Security Standard  
Protection of Personal Data Security Controls  
P/S Security Policy

The Privacy Official is responsible for resolving any conflicts between the terms of the HIPAA Security Policy and any other Dow policy.

## **C. Administrative Safeguards**

### **1. Security Management Process**

As of April 20, 2005, the Security Official has determined that the IS security policies currently in place reasonably and sufficiently prevent, detect, contain and correct security violations regarding ePHI. These policies are listed in Article XII, Section B of this Privacy Policy, with links to the applicable websites or webpages. In particular, please refer to the “Dow Policy on Protection of Personal Employee Data” and the “Protection of Personal Data Security Controls at The Dow Chemical Company”.

As a general rule, Responsible Persons who need to access ePHI in the normal course of their duties may access such ePHI only on authorized computers in accordance with the Dow’s Corporate Policy on Computer Systems and Telecommunications Security. Each such computer will be assigned and maintained in accordance with this security policy, including applicable procedures regarding password protection, periodic back-up, virus protection, etc. All computer files and databases containing PHI received, created or maintained by the Health Plan in electronic form which require access by more than one Responsible Person or which may be accessed by a Business Associate or Covered Participant are required to be maintained on a secure network, and all Dow security, firewall, data back up, access authorization and other policies and security procedures applicable to confidential material on a Dow extranet network will apply. Access to files, databases and other ePHI are password protected and are available only to Responsible Persons who have been trained as to their HIPAA privacy requirements.

PHI in electronic form (e.g., e-mail, databases and computer files containing ePHI) will be maintained and stored in a secure manner by the Health Plan and/or by a Business Associate which has entered into an agreement with the Health Plan maintain appropriate safeguards of ePHI that are comparable to, or at least as stringent as those set forth below. Electronic Transmissions containing PHI must, to the extent reasonably possible, be protected so that they cannot be intercepted by parties other than the intended recipient, or accessed by unauthorized users.

**a) Risk analysis and management.**

As of April 20, 2005, the Security Official, on behalf of the Health Plans, and in conjunction with Dow's Information Systems Department ("IS"), has completed an assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of ePHI held by the Health Plans at Dow. Transmissions of ePHI must go through the risk assessment process described in the IS policy, "Dow Cybersecurity Strategy". Risk assessments are maintained by IS. IS has implemented security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level as identified in the "Dow Cybersecurity Strategy" process.

As of April 20, 2005, the Security Official has confirmed that the Health Plans have either amended their business associate agreements (or entered into new business associate agreements), or have completed negotiations with respect to such agreements, to address the security of ePHI created, received and maintained by such Business Associates. The Business Associates have agreed to comply with the requirements of 45 CFR Part 164, including a security risk assessment.

b) Sanction Policy - Appropriate sanctions against workforce members who fail to comply with the security policies of the Health Plan will be administered. As noted in the "Corporate Policy on Computer Systems and Telecommunications Security", 'Violations of this policy may subject the person responsible to disciplinary action up to and including termination of employment'. Additional sanctions information can be found in the "Information Security Policy Enforcement Process"

c) Information System Activity Review - Procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports are in place. IS maintains logs and monitors activity in the systems that host the applications and data that contain ePHI. Activity monitors include unauthorized access, profile changes, password resets, new account creations, unauthorized account creations, etc. These activities are monitored on a specific schedule, depending on the hardware or systems usage.

## **2. Security Official**

The Security Official is responsible for this Section XII of the Privacy Policy. The Security Official is the same person as the Privacy Official.

## **3. Workforce Security**

IS has implemented the policy, "Protection of Personal Data Security Controls at The Dow Chemical Company", and the Privacy Official has implemented the HIPAA Privacy Policy, both of which are designed to ensure that the members of its workforce who need to have access to ePHI have access, and to prevent those workforce members who should not have access from obtaining access. These policies address the following, as well as other issues:

- (a) Procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed.
- (b) Procedures to determine that the access of a workforce member to ePHI is appropriate.
- (c) Procedures for terminating access to ePHI when the employment of a workforce member ends or as otherwise is appropriate.

## **4. Information Access Management**

IS has implemented the policies, "P/S Security Policy" and in the "Dow Workstation DWS2003 Security Standard". These policies provide procedures for authorizing access to ePHI. Access is only granted to authorized users as documented in the Dow Workstation DWS2003 Security Standard. These standards include documentation on the following:

- a) Policies and procedures for granting access to ePHI, for example, through access to a workstation, transaction, program, process or other mechanism.
- b) Policies and procedures that based upon the entity's access authorization policies, establish, document, review and modify a user's right of access to a workstation, transaction, program, or process. These are documented in the Identification and Authentication standard as set forth in the Information Security Standards.

## **5. Security Awareness and Training**

IS has implemented security awareness and training programs for all members of its workforce (including Responsible Persons). There are programs and mandatory courses that feature training in the areas of information security, information handling and records management. The courses are as follows:

Information and Records Management Overview (CP-2143, Learn@dow.now).

Protection of Personal Employee Data (Global Ethics and Compliance (CP-0837, Learn@dow.now).

In addition, IS provides:

- a) Periodic security updates and posts reminders on the Company intranet and broadcasts such updates and reminders through its' Newslane feature. [Click here for a sample article.](#)
- b) Employees (including Responsible Persons) information about procedures for guarding against, detecting, and reporting malicious software. [Click here to access the Information Security web site](#), or [here to access the Virus Protection Policy web site.](#)
- c) Procedures for creating, changing, and safeguarding passwords. [Click here to access the corporate Password security policy.](#)
- d) Procedures for monitoring log-in attempts and reporting discrepancies. Please see Article XII, C., 1, c). for more details.

## **6. Security Incident Procedures**

IS has established and implemented the "Information Security Center Investigation Process" and the "Virus Protection Policy", which are designed to address security incidents. Under these policies, IS will respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the Health Plan; and document security incidents and their outcomes.

## **7. Contingency Plan**

IS has established and implemented "The Dow Chemical Company Corporate Policy on Computer Systems and Telecommunications Security" policy. Under such policy:

- a) A Data backup plan has been established and implemented across the company. On at least a daily basis, full back-ups of all major systems, and most Dow workstations are performed. These create and maintain retrievable exact copies of all data, including any ePHI.
- b) A Disaster recovery plan exists for all major Dow systems, with procedures to restore any lost data, as well as procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode. Please see Exhibit E for a summary of the most recent integrated Disaster Recovery Exercise for the PeopleSoft system, which hosts all of the ePHI for the Company.

c) The Disaster Recovery Plan includes procedures for periodic testing and revision of contingency plans. These plans also address the assessment of the relative criticality of specific applications and data in support of other contingency plan components.

## **8. Evaluation**

Periodic technical and non-technical evaluations, based initially upon the standards implemented under the Security Regulations, and subsequently, in response to environmental or operational changes will be conducted. Major changes to systems and/or environments trigger the methodology that triggers the Dow's Risk Assessment process. See the I/S Methodology Workbench at: [I/S Methodology Workbench \(http://isworkbench.intranet.dow.com/default.htm\)](http://isworkbench.intranet.dow.com/default.htm) for details.

## **9. Business Associate Contracts**

As of April 20, 2005, the Security Official has confirmed that the Health Plans have amended their business associate agreements (or entered into new business associate agreements) to address the security of ePHI created, received and maintained by such Business Associates. The Business Associates have agreed to comply with the requirements of 45 CFR Part 164, including a security risk assessment.

## **D. Physical Safeguards**

**1. Facility Access Controls.** – See Article V. B regarding restrictions to facility access.

a) **Contingency Operations & Facility and Security Plan & Access Control and Validation**—Persons regularly employed on the premises, including the premises that support restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency, will be issued and display electronic or photographic “key cards” that permit the tracking of access into the building. Key cards, pass keys or other means of access will be issued and maintained in accordance with Dow's building security policies. Visitors entering the building will be required to sign in and show valid identification to building security personnel in accordance with Dow's building security policies. Entry will be denied to any person who does not have legitimate business on the premises, thus preventing unauthorized physical access, tampering, and theft.

For additional information on access to the facilities that house the physical equipment (storage devices, servers, etc.) please refer to the 2050 Physical Security Sarbanes-Oxley (SOX) audit results. This lists a series of control activity questions around physical security of the Dow computer infrastructure. (See Appendix xx).

b) **Maintenance Records** - Procedures are in place to document repairs and modifications to the physical components of a facility that are related to security (for example, hardware, walls, doors, and locks.). These are tracked by the building maintenance work order system. Please see the Emergency Services & Security information located at: Emergency Services and Security Expertise Center ([http://ehs.intranet.dow.com/TEAMSANDGROUPS/ESS/ess\\_ec.htm#General%20Information](http://ehs.intranet.dow.com/TEAMSANDGROUPS/ESS/ess_ec.htm#General%20Information))

**2. Workstation Use** – IS has established and implemented the “Dow Workstation DWS2003 Security Standard”, which specifies the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surrounding of a specific workstation or class of workstation that can access ePHI.

**3. Workstation Security** – IS has established and implemented the “Dow Workstation DWS2003 Security Standard”, which specifies physical safeguards such as locks on devices for all workstations that access ePHI and addresses access restriction through personal passwords.

**4. Device and Media Controls** – Dow implements policies and procedures that govern the receipt and removal of hardware and electronic media that contain EPHI into and out of a facility, and the movement of these items within the facility.

a. Disposal – Policies and procedures are in place to address the final disposition of ePHI, and/or hardware or electronic media on which it is stored. The disposal of workstations is covered under the Compliance Guidelines of the Corporate Policy on Computer Systems and Telecommunications Security which can be found [here](#).

b. Media Reuse – Procedures have been implemented for removal of ePHI from electronic media before the media are made available for re-use. For more information, please consult the Dow Records Management Policy, specifically, the detailed guidance for handling disposing Dow information. This can be found by clicking the link [here](#).

c. Accountability – Dow maintains records of the movements of hardware and electronic media and any person responsible for such movement as outlined in the Dow Workstation transfer policy, and the Corporate Policy on Computer Systems and Telecommunications Security.

d. Data Backup and Storage. – Procedures are in place to create a retrievable, exact copy of EPHI, when needed, before movement of equipment. This is addressed in the daily back-ups of Dow workstation data, and in the

Information Security Standards and the Change Integration and Implementation Procedures.

## **E. Technical Safeguards**

**1. Access Control** - Dow has implemented technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights. In general, roles based access controls are in force for the systems that contain ePHI.

a. In accordance with Dow IS policies, a unique user identification is assigned to all Responsible Persons. This includes the assignment of a unique name and/or number for identifying and tracking user identity.

b. Emergency access procedures are in place to insure necessary ePHI can be obtained during an emergency. Also see Article XII, C, 7. Contingency Plans.

c. Users are automatically logged off the system after a period of 30 minutes of inactivity. Workstation policy calls for users to have screensavers established to prevent unauthorized users access to the system when they are not at their workstations.

d. ePHI that is transmitted outside of Dow is encrypted to prevent unauthorized access. When using open networks (i.e., the internet or dial-in lines), the PHI will be encrypted before sending in order to avoid interception by parties other than the intended recipient; or for non-open networks, either access control (password protection) or encryption will be used to prevent parties other than the intended recipient from intercepting messages.

**2. Audit Controls** – Dow has implemented hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI. See Article XII.C.1.c) for details.

**3. Integrity** – Only Responsible Persons are allowed to modify records in the system that contain ePHI, as Responsible Persons are the only persons permitted access to such ePHI. Policies such as the Dow Records Management Policy are in place to insure that destruction of ePHI is only carried out in accordance with these policies.

**4. Mechanism to authenticate ePHI** – IS has installed electronic mechanisms such as encryption and secure transmission protocols to corroborate that ePHI transmitted to or from Dow's systems has not been altered or destroyed in an unauthorized manner. This also includes financial and audit controls on files to insure that the data is accurately maintained.

**5. Person or entity authentication** - Access to PHI in electronic form is restricted to Responsible Persons. Responsible Persons whose job duties do not require use or disclosure of PHI, but who are located in areas where ePHI is kept or have access to ePHI through the Dow Global Human Resources Information System (GHRIS), are trained not to look at, or use or disclose PHI. Failure to comply with this requirement may subject such Responsible Person to disciplinary action up to and including termination of employment. Please refer to the Administrative Safeguards as noted in this policy, Section XII.C.

**6. Transmission security** - Technical security measures are in place that guard against unauthorized access to ePHI that is being transmitted over an electronic communications network. Internal (“Dow”) communications are maintained within Dow’s firewall and are secure from unauthorized access. Those that are transmitted outside Dow are subject to encryption as specified in V.C.2. of this policy.

a. Integrity controls –Security measures are in place to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of. Normal network protocol means, as implemented by the Dow IS function, are in place to adequately protect the transmitted data.

b. Encryption – As previously stated a mechanism is in place to encrypt ePHI whenever deemed appropriate. See Sect V.C.2 of this policy.

## **EXHIBIT A: Notice of Privacy Practices**

---

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

**Effective Date of Notice:** April 14, 2003.

The Dow Chemical Company Medical Care Program, The Dow Chemical Company Retiree Medical Care Program, The Dow Chemical Company Dental Assistance Program, The Dow Chemical Company Retirement Health Care Assistance Plan (RHCAP), The Dow Chemical Company Health Care Reimbursement Account, The Dow Chemical Company Executive Physical Examination Program, the Union Carbide Corporation Retiree Medical Care Program (renamed), Rohm and Haas Company Health and Welfare Plan (collectively referred to in this document as the “Program”) are required by law to take reasonable steps to ensure the privacy of your personally identifiable health information and to inform you about:

- the Program’s uses and disclosures of Protected Health Information (PHI);
- your privacy rights with respect to your PHI;
- the Program’s duties with respect to your PHI;
- your right to file a complaint with the Program and to the Secretary of the U.S. Department of Health and Human Services; and
- the person or office to contact for further information about the Program’s privacy practices.

The term “Protected Health Information” (PHI) includes all individually identifiable health information transmitted or maintained by the Program.

This notice does not apply to information that has been de-identified. De-identified information is information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information. In addition, the Program may use or disclose “summary health information” to the plan sponsor for obtaining premium bids or modifying, amending or terminating the group health Program, which summarizes the claims history, claims expense or type of claims experienced by individuals for whom a Program sponsor has provided health benefits under a group health Program; and from which identifying information has been deleted in accordance with HIPAA.

## Section 1. Notice of PHI Uses and Disclosures

---

### **Required PHI Uses and Disclosures:**

Upon your request, the Program is required to give you access to certain PHI in order to inspect and copy it. Use and disclosure of your PHI may be required by the Secretary of the Department of Health and Human Services to investigate or determine the Program's compliance with the privacy regulations.

Uses and disclosures to carry out treatment, payment and health care operations:

The Program and its business associates will use PHI without your consent, authorization or opportunity to agree or object to carry out treatment, payment and health care operations. The Program also will disclose PHI to the applicable Plan Sponsor<sup>1</sup> for purposes related to treatment, payment and health care operations. As of April 14, 2003, the Plan Sponsors have amended the plan document to protect your PHI as required by federal law.

*Treatment* is the provision, coordination or management of health care and related services. It also includes but is not limited to consultations and referrals between one or more of your providers. For example, The Dow Chemical Company Medical Care Program may disclose to a treating orthopedic specialist the name of your treating family physician so that the orthopedic specialist may ask for your X-rays from the treating family physician.

*Payment* includes but is not limited to actions to make coverage determinations and payment (including billing, claims management, subrogation, plan reimbursement, reviews for medical necessity and appropriateness of care and utilization review and preauthorizations). For example, The Dow Chemical Company Medical Care Program may tell a doctor whether you are eligible for coverage or what percentage of the bill will be paid by the Program.

*Health care operations* include but are not limited to quality assessment and improvement, reviewing competence or qualifications of health care professionals, underwriting, premium rating and other insurance activities relating to creating or renewing insurance contracts. It also includes disease management, case management, conducting or arranging for medical review, legal services and auditing functions including fraud and abuse compliance programs, business planning and development, business management and general administrative activities. For example, The Dow Chemical Company Medical Care Program may use information about your claims to refer you to a disease management program, project future benefit costs or audit the accuracy of its claims processing functions.

### **Uses and disclosures that require your written authorization:**

In general, your written authorization will be obtained before the Program will use or disclose psychotherapy notes about you from your psychotherapist. Psychotherapy notes are separately

---

<sup>1</sup> The Plan Sponsor is The Dow Chemical Company for the following plans: for The Dow Chemical Company Medical Care Program, The Dow Chemical Company Retiree Medical Care Program, The Dow Chemical Company Dental Assistance Program, The Dow Chemical Company Retirement Health Care Assistance Plan (RHCAP), The Dow Chemical Company Health Care Reimbursement Account, and The Dow Chemical Company Executive Physical Examination Program. The Plan Sponsor is Union Carbide Corporation, a wholly-owned subsidiary of The Dow Chemical Company, for the following plan: Union Carbide Corporation Retiree Medical Care Program.

filed notes about your conversations with your mental health professional during a counseling session. They do not include summary information about your mental health treatment. The Program may use and disclose such notes when needed by the Program to defend against litigation filed by you.

### **Uses and disclosures that require that you be given an opportunity to agree or disagree prior to the use or release**

Disclosure of your PHI to family members, other relatives and your close personal friends is allowed if:

- the information is directly relevant to the family or friend's involvement with your care or payment for that care; and
- you have either agreed to the disclosure or have been given an opportunity to object and have not objected.

### **Uses and disclosures for which consent, authorization or opportunity to object is not required:**

Use and disclosure of your PHI is allowed without your consent, authorization or request under the following circumstances:

1. When required by law.
2. When permitted for purposes of public health activities, included when necessary to report product defects, to permit product recalls and to conduct post-marketing surveillance. PHI may also be used or disclosed if you have been exposed to a communicable disease or are at risk of spreading a disease or condition, if authorized by law.
3. When authorized by law to report information about abuse, neglect or domestic violence to public authorities if there exists a reasonable belief that you may be the victim of abuse, neglect or domestic violence. In such case, the Program will promptly inform you that such a disclosure has been or will be made unless that notice would cause a risk of serious harm. For the purpose of reporting child abuse or neglect, it is not necessary to inform the minor that such a disclosure has been or will be made. Disclosure may generally be made to the minor's parents or other representatives although there may be circumstances under federal or state law when the parents or other representatives may not be given access to the minor's PHI.
4. The Program may disclose your PHI to a public health oversight agency for oversight activities authorized by law. This includes uses or disclosures in civil, administrative or criminal investigations; inspections; licensure or disciplinary actions (for example, to investigate complaints against providers); and other activities necessary for appropriate oversight of government benefit programs (for example, to investigate Medicare or Medicaid fraud).
5. The Program may disclose your PHI when required for judicial or administrative proceedings. For example, your PHI may be disclosed in response to a subpoena or discovery request provided certain conditions are met. One of those conditions is that satisfactory assurances must be given to the Program that the requesting party has made a good faith attempt to provide written notice to you, and the notice provided

- sufficient information about the proceeding to permit you to raise an objection and no objections were raised or were resolved in favor of disclosure by the court or tribunal.
6. When required for law enforcement purposes (for example, to report certain types of wounds).
  7. For law enforcement purposes, including for the purpose of identifying or locating a suspect, fugitive, material witness or missing person. Also, when disclosing information about an individual who is or is suspected to be a victim of a crime but only if the individual agrees to the disclosure or the covered entity is unable to obtain the individual's agreement because of emergency circumstances. Furthermore, the law enforcement official must represent that the information is not intended to be used against the individual, the immediate law enforcement activity would be materially and adversely affected by waiting to obtain the individual's agreement and disclosure is in the best interest of the individual as determined by the exercise of the Program's best judgement.
  8. When required to be given to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death or other duties as authorized by law. Also, disclosure is permitted to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to the decedent.
  9. The Program may use or disclose PHI for research, subject to conditions.
  10. When consistent with the applicable law and good standards of ethical conduct if the Program, in good faith, believes the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and the disclosure is to a person reasonably able to prevent or lessen the threat, including the target of the threat.
  11. When authorized by and to the extent necessary to comply with workers' compensation or other similar programs established by law. Except as otherwise indicated in this notice, uses and disclosures will be made only with your written authorization subject to your right to revoke such authorization.

## **Section 2. Rights of Individuals**

---

### **Right to Request Restrictions on PHI Uses and Disclosures:**

You may request the Program to restrict uses and disclosures of your PHI to carry out treatment, payment or health care operations, or to restrict uses and disclosures to family members, relatives, friends or other persons identified by you who are involved in your care or payment for your care. However, the Program is not required to agree to your request. The Program will accommodate reasonable requests to receive communications of PHI by alternative means or at alternative locations. You or your personal representative will be required to complete a form to request restrictions on uses and disclosures of your PHI. Such requests should be made to the following person: Privacy Official; ERISA Health Plans; Employee Development Center, Midland, MI 48674

## **Right to Inspect and Copy PHI:**

You have a right to inspect and obtain a copy of your PHI contained in a “designated record set,” for as long as the Program maintains the PHI.

“*Protected Health Information*” (PHI) includes all individually identifiable health information transmitted or maintained by the Program, regardless of form.

“*Designated Record Set*” includes the medical records and billing records about individuals maintained by or for a covered health care provider; enrollment, payment, billing, claims adjudication and case or medical management record systems maintained by or for a health plan; or other information used in whole or in part by or for the covered entity to make decisions about individuals. Information used for quality control or peer review analyses and not used to make decisions about individuals is not in the designated record set. The requested information will be provided within 30 days if the information is maintained on site or within 60 days if the information is maintained offsite. A single 30-day extension is allowed if the Program is unable to comply with the deadline. You or your personal representative will be required to complete a form to request access to the PHI in your designated record set. Requests for access to PHI should be made to the following person: Privacy Official; ERISA Health Plans; Employee Development Center, Midland, MI 48674. If access is denied, you or your personal representative will be provided with a written denial setting forth the basis for the denial, a description of how you may exercise those review rights and a description of how you may complain to the Secretary of the U.S. Department of Health and Human Services.

## **Right to Amend PHI:**

You have the right to request the Program to amend your PHI or a record about you in a designated record set for as long as the PHI is maintained in the designated record set. The Program has 60 days after the request is made to act on the request. A single 30-day extension is allowed if the Program is unable to comply with the deadline. If the request is denied in whole or in part, the Program must provide you with a written denial that explains the basis for the denial. You or your personal representative may then submit a written statement disagreeing with the denial and have that statement included with any future disclosures of your PHI. Requests for amendment of PHI in a designated record set should be made to the following person: Privacy Official; ERISA Health Plans; Employee Development Center, Midland, MI 48674. You or your personal representative will be required to complete a form to request amendment of the PHI in your designated record set. You must make your request for amendment in writing, provide the name of the applicable benefit plan you are requesting the amendment under, and provide the reason(s) to support the amendment you are requesting.

## **The Right to Receive an Accounting of PHI Disclosures:**

At your request, the Program will also provide you with an accounting of disclosures by the Program of your PHI during the six years prior to the date of your request. However, such

accounting need not include PHI disclosures made: (1) to carry out treatment, payment or health care operations; (2) to individuals about their own PHI; (3) pursuant to an individual's authorization; or (4) prior to the compliance date. If the accounting cannot be provided within 60 days, an additional 30 days is allowed if the individual is given a written statement of the reasons for the delay and the date by which the accounting will be provided. If you request more than one accounting within a 12-month period, the Program may charge a reasonable, cost-based fee for each subsequent accounting.

### **The Right to Receive a Paper Copy of This Notice Upon Request:**

To obtain a paper copy of this Notice contact the following person: Health Insurance Portability and Accountability Act (HIPAA) Privacy Official for ERISA Health Plans; Employee Development Center, Midland, MI 48674

### **A Note About Personal Representatives:**

You may exercise your rights through a personal representative. Your personal representative will be required to produce evidence of his/her authority to act on your behalf before that person will be given access to your PHI or allowed to take any action for you. Proof of such authority may take one of the following forms:

- a power of attorney for health care purposes, notarized by a notary public;
- a court order of appointment of the person as the conservator or guardian of the individual; or
- an individual who is the parent of a minor child.

The Program retains discretion to deny access to your PHI to a personal representative to provide protection to those vulnerable people who depend on others to exercise their rights under these rules and who may be subject to abuse or neglect. This also applies to personal representatives of minors.

### **Section 3. The Program's Duties**

---

The Program is required by law to maintain the privacy of PHI and to provide individuals (participants and beneficiaries) with notice of its legal duties and privacy practices. This notice is effective beginning April 14, 2003 and the Program is required to comply with the terms of this notice on and after that date. However, the Program reserves the right to change its privacy practices and to apply the changes to any PHI received or maintained by the Program prior to and after that date. If a privacy practice is changed, a revised version of this notice will be provided participants and beneficiaries for whom the Program still maintains PHI. The notices may be provided in the Choices enrollment brochures and updated versions of the summary plan descriptions, or other appropriate means of communication. Any revised version of this notice will be distributed within 60 days of the effective date of any material change to the uses or disclosures, the individual's rights, the duties of the Program or other privacy practices stated in this notice.

### **Minimum Necessary Standard:**

When using or disclosing PHI or when requesting PHI from another covered entity, the Program will make reasonable efforts not to use, disclose or request more than the minimum amount of PHI necessary to accomplish the intended purpose of the use, disclosure or request, taking into consideration practical and technological limitations. However, the minimum necessary standard will not apply in the following situations:

- disclosures to or requests by a health care provider for treatment;
- uses or disclosures made to the individual;
- disclosures made to the Secretary of the U.S. Department of Health and Human Services;
- uses or disclosures that are required by law;
- uses or disclosures authorized by the individual; and
- uses or disclosures that are required for the Program's compliance with legal regulations.

### **Section 4. Your Right to File a Complaint With the Program or the HHS Secretary**

---

If you believe that your privacy rights have been violated, you may complain to the Program in care of the following person: Privacy Official; ERISA Health Plans; Employee Development Center, Midland, MI 48674. You may file a complaint with the Secretary of the U.S. Department of Health and Human Services, Hubert H. Humphrey Building, 200 Independence Avenue S.W., Washington, D.C. 20201. The Program will not retaliate against you for filing a complaint.

### **Section 5. Whom to Contact at the Program for More Information**

---

If you have any questions regarding this notice or the subjects addressed in it, you may contact the following person: Privacy Official; ERISA Health Plans; Employee Development Center, Midland, MI 48674

**CONCLUSION:** PHI use and disclosure by the Program is regulated by a federal law known as HIPAA (the Health Insurance Portability and Accountability Act.) You may find these rules at 45 *Code of Federal Regulations* parts 160 and 164. This notice attempts to summarize the regulations. The regulations will supersede any discrepancy between the information in this notice and the regulations.

**Exhibit B**

**Privacy Official and Responsible Person Delegations**

**(1) Appointments**

<b>PRIVACY OFFICIAL NAME</b>	<b>EFFECTIVE DATE OF APPOINTMENT</b>
J. Michael Dizer	April 14, 2003

**(2) Responsible Person Designations**

**LEVEL I**

Manager, Resource Center

Privacy Official

HR Legal Counsel for Welfare Plans

Senior Design Leader, Strategic Center

Director, Global Benefits, Strategic Center

Manager, TDCC Medical Care Program

Manager, TDCC Retiree Medical Care Program

Manager, TDCC Insured Health Program

Manager, TDCC Dental Assistance Program

Manager, TDCC RHCAP

C&B Technologist Leader, TDCC RHCAP

Manager, TDCC Health Care Reimbursement Account

Manager, Union Carbide Corporation Retiree Medical Care Program

Manager, Union Carbide Corporation Insured Retiree Health Program

Administrator of Executive Physical Examination Program (at both the claims administrator level and the appellate level)

Retirement Board

**LEVEL II**

Resource Center employees directly supervised by the Manager, Resource Center

Employees directly supervised by the Privacy Official

Legal Department employees directly supervised by HR Legal Counsel for Welfare Plans

Strategic Center employees directly supervised by the Senior Design Leader, Strategic Center

Strategic Center employees directly supervised by the Director, Global Benefits, Strategic Center

Retiree Service Center

H.R. Service Center

Payroll

Information Systems

Internal Auditors who are directly involved with auditing a health plan

## Exhibit C

### Routine Disclosures to Business Associates

The following table sets forth the routine disclosures of PHI to Business Associates. All of the transactions listed below have been determined to comply with the Minimum Necessary requirement of Article IV. Any deviations from this list of routine transactions must be approved by a Level I Responsible Person. If, after referring to the tables below, a Responsible Person is unsure about whether or what PHI can be disclosed to a Business Associate, the Responsible Person should contract his or her supervisor or the Privacy Official.

<b>BUSINESS ASSOCIATE RECEIVING PHI</b>	<b>REASON FOR DISCLOSURE OF PHI BY HEALTH PLANS</b>	<b>PHI PROVIDED</b>
Aetna	Medical Plan and Prescription Drug third party administration	Enrollment and Eligibility data
Delta Dental	Dental Plan third party administrator	Enrollment and Eligibility data
Watson Wyatt	Health care operations, including calculating claims liability, premiums, and FAS 106 liability, as well as audit functions, non-discrimination testing, consulting on plan design	Enrollment and Eligibility data. In addition, the Health Plans' other Business Associates provide Claims data to Watson Wyatt.
MedStat	Data analysis	Enrollment and eligibility data. In addition, the Health Plans' other Business Associates provide Claims data to Medstat.
Cobra Serv	Third party administration of COBRA benefits	Qualifying event, Enrollment and Eligibility data
Medco	Third party administration of prescription drug benefits under medical plans through December 31, 2002, and run out claims	Enrollment and Eligibility data
IRG	Third party administration of mental health and substance abuse claims	Enrollment and Eligibility data
UniCare	Third party administration of medical plans through December 31, 2002, and run out claims	Enrollment and Eligibility data
UltraLink	HMO/DMO network manager	Enrollment and Eligibility data

<b>BUSINESS ASSOCIATE RECEIVING PHI</b>	<b>REASON FOR DISCLOSURE OF PHI BY HEALTH PLANS</b>	<b>PHI PROVIDED</b>
Accenture	Computer systems software contractor	Access to GHRIS, GHRIS data
Deloitte & Touche	External auditor for RHCAP. Potential auditor if any trust is used to pay medical claims for any of the other Health Plans.	Enrollment, Eligibility, and claims data.
Mercer	Health care operations	Enrollment and Eligibility data. In addition, the Health Plans' other Business Associates provide Claims data to Mercer.
Health & Productivity Corporation of America	Health care operations	Enrollment and Eligibility data. In addition, the Health Plans' other Business Associates provide Claims data to Mercer.
Social Security Disability Consultants and Disability Services, Inc. (SSDC/DSI),	Third party administrator to administer coordination of benefits between Medicare and the health plans.	Enrollment and Eligibility data. In addition, the Health Plans' other Business Associates provide Claims data to SSDC/DSI.
EDS	Answering general questions concerning the health plans	Enrollment and Eligibility data
Arnold Center	Collating documents and stuffing envelopes	Enrollment information and data

## **Exhibit D**

### **Areas Where Access Is Restricted to Responsible Persons**

Z-0 South, 2020 Building, Midland, MI

Employee Development Center, 2<sup>nd</sup> Floor, Midland, MI

Building 1610, Midland, MI

9008 Building, Midland, MI

39 Old Ridgebury Rd., Danbury, CT

UNRESTRICTED - May be shared with anyone

Content Owner: J. M. Dizer  
Last Updated: April 20, 2005

# Exhibit E

## EXECUTIVE SUMMARY

On September 16th, Teams from The Dow Chemical Company and IBM conducted a fifty-six hour recovery exercise which tested the ability to recover all Enterprise Critical Systems environments simultaneously using the IBM Sterling Forest, New York and IBM Southfield, Michigan facilities.

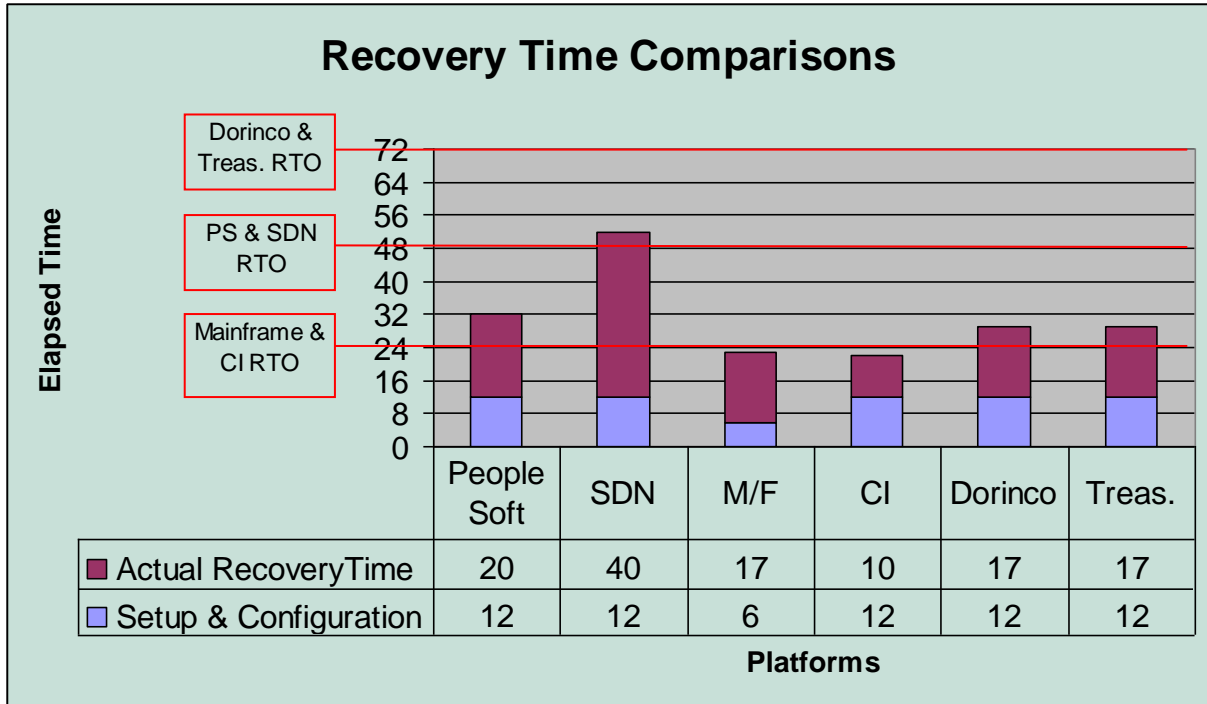
This exercise was a solid step forward and a success on many levels. There were a few issues resulting from this simultaneous recovery objective. However, these several lessons learned will enhance and strengthen the recovery program.

This exercise went further into both infrastructure and application (data) validation, on all platforms, than we have experienced to date. This is a significant step forward in full recoverability for The Dow Chemical Company.

The following is a detailed description of the effort undertaken:

- ✓ All four Mainframe images were successfully recovered. The Independent Test Team validated this assessment. DPRS as well as the new DB2 V.8 database were successfully recovered and tested. External commuter connections to Kleinschmidt, Geis, Vucom and IBM were established and tested successfully.
- ✓ The Global Reporting environment experienced hardware delays. This resulted in our failure to meet the Recovery Time Objective (RTO). We did however fully recover the environment. Interface and data movement testing was successfully exercised. Both the Dow and IBM subject matter experts are working to determine the cause of the difficulties encountered.
- ✓ Business Objects and Power Play reporting tools were successfully recovered and tested.
- ✓ The network recovery concluded with the team establishing extranet and firewall environments. This new environment allowed the Treasury team to establish successful connections to both Swift and systems hosting in IBM Raleigh, NC. All of these were new accomplishments for our program.
- ✓ The first effort to exercise the Dorinco Disaster Recovery Plan was successful. After diagnosing early problems, Tech Management was able to successfully execute the Synergy application from Midland.
- ✓ The Peoplesoft recovery was completed successfully. The Peoplesoft environment did experience problem, but are being addressed. Contingency plans were tested to ensure the movement of this data could occur manually during a true disaster.
- ✓ The Customer Service recovery in Southfield, MI completed successfully. The team was able to reroute production fax and telephone lines into IBM's Southfield facility. The team also built 100 Dow Workstations to simulate the work area recovery for a disaster that may have impacted 2040 or 9008 buildings. The Customer Interface Team also was able to access the recovered SAP environment in Sterling Forest where they simulated creating orders and processing several types of transactions.

Attachment



Legend

RTO = Recovery Time Objective (Failure to Recovery)

- PeopleSoft = People Systems
- SDN = Share Data Network (Dow Reporting Environment)
- M/F = Mainframe (SAP, Maintenance and Purchasing Systems)
- CI = Customer Interface and Customer Service facilities
- Treas. = New Treasury Systems