Bristol Myers Squibb™

BMS UNITED STATES PRIVACY NOTICE

1. INTRODUCTION

This United States Privacy Notice ("Privacy Notice" or "Notice") explains how Bristol-Myers Squibb Company ("BMS," or "we," or "us," or "our") collects and uses personal information or personal data ("personal information") about you when you interact with us online, including on our websites (including product websites for our medicines) and mobile applications, offline, in the context of our business activities. It also informs you about your privacy rights and the measures and processes we put in place to protect your data. The bottom of this Notice contains information specific to job applicants. We also operate under the name(s) as described in our 10-K.

2. SCOPE AND DEFINITIONS

If you are an employee (or consultants, contractors, interns, or third parties as defined in this Notice – collectively called "workers"), please refer to the Employee Privacy Notice wherein such terms are defined. If you are a supplier or business partner, please refer to your contractual agreements with BMS for additional information.

In this Notice, we refer to you as "you" or "your." We use the term "Processing" or "Use" when we refer to the access, collection, recording, organization, structuring, retrieval, disclosure, storage, transfer, deletion or otherwise use of your Personal Information.

3. WHY WE PROVIDE THIS U.S. PRIVACY NOTICE

This US Privacy Notice explains our practices with respect to the collection and use of personal information and describes the rights you may have with respect to your personal information under applicable US Privacy Law. As used in this Notice, "US Privacy Law" collectively refers to the various US federal and comprehensive state data privacy statutes that govern the collection, use, and disclosure of personal information of Consumers residing in the United States. All defined terms in this Notice have the same meanings as those set forth under US Privacy Law. Because these definitions may vary from state to state, the specific definitions and rights that apply to you are those defined by the laws of the state where you reside.

4. CONSENT

By using this website and otherwise interacting with us, you agree to the terms of our Legal Notice and this Notice.

5. CONSUMER HEALTH DATA

To see our separate Consumer Health Data Privacy Notices, please read our Washington Consumer Health Data Privacy Notice if you are a Washington resident or if your data is processed there, or our Nevada Consumer Health Data Privacy Notice if you are a Nevada resident or your data is processed there. Each notice describes your rights under the applicable state's consumer health data privacy laws and explains how to exercise them.

6. NOTICE AT COLLECTION: PERSONAL INFORMATION WE COLLECT

We collect the following categories of personal information:

- **Personal identifiers:** Full name, personal or professional postal and/or email address, phone number, governmental ID information, date of birth, IP address, account login information and password, pseudonymous identifiers, mobile advertising ID, social security number, IP address, mobile ad ID, social media handles

- **Protected class information:** Gender, race and ethnicity information, age over 40, sexual orientation, genetic information, sex

- **Insurance information:** Health insurance information

- **Health information**: Information about your health status or condition; dietary preferences or restrictions (such as food allergies), special conditions or disabilities when attending an event; genetic data to provide our therapies to you

- **Financial information:** Bank account and payment information; information used to verify income or account balance information (for patient support programs)

- **Commercial and financial information**: records of products ordered or considered; other purchasing or consuming histories and tendencies

- **Professional and educational information**: job title, information about your employer relating to individuals we interact with in a business setting; self-selected descriptions of your professional, caregiver or student status in inquiry forms submitted to us

- **Internet or other electronic activity information**: Your device and browser type, operating systems, device ID, your browsing and search history on our website and other sites; data captured by cookies and similar tracking technologies regarding your interaction with our websites and mobile apps (read our cookies section [please hyperlink below)

- **Geolocation information:** geolocation information

- **Audio, visual information**: recordings of calls made to our customer service, product reporting, and medical information phone lines; photographs taken for security purposes when you visit our facilities

- **Inferences drawn from personal information we collect**: In some cases, we may create inferences or profiles from personal information we collect about you

- **Sensitive personal information**: In some situations, we collect sensitive personal information about you. Depending upon the country in which you reside and the particular context for the collection of such personal information, this may include the following information, which we have already identified above: Data revealing race or ethnicity; National ID, passport number, social security number, driver's license number; data related to sex life or sexual orientation; precise geolocation; health or disability information; dietary preferences that may reveal your religion or philosophical beliefs; genetic information

We have collected the same categories of personal information in the 12 months prior to the date of this Privacy Notice.

7. Notice at Collection - Purposes for Collection of Personal Information

We collect the categories of personal information identified for the following purposes and have done so in the 12 months prior to the date of this Notice:

Categories of Personal Information	Purposes for Collection
Personal identifiers: Full name, personal or professional postal and/or email address, phone number, governmental ID information, date of birth, account login information and password, social security number Protected class information: Gender, race and ethnicity, age over 40, sexual orientation, genetic information, sex Financial information: Information used to verify income or account balance information (for patient support programs) Internet or other electronic activity information: your device and browser type, operating systems, device ID Audio information: recordings of customer service calls Health data: Health data needed to provide our products and services	To provide our products and services, including our drug therapies and medical devices, to provide patient advocacy and support activities, and respond to your inquiries
Personal identifiers: Full name, personal or professional postal and/or email address, phone number, governmental ID information, date of birth, account login information and password, social security number Protected class information: Gender, race and ethnicity, age over 40 Financial information: Information used to verify income or account balance information (for patient support programs) Internet or other electronic activity information: your device and browser type, operating systems, device ID Audio information: recordings of customer service calls Health data: Health data needed to provide our products and services; allergy information when selecting food choices at events	Managing our relationship with you, including to respond to your questions, when you attend or speak at events we host
Personal identifiers: Full name, personal or professional postal and/or email address, phone number, governmental ID information, date of birth, IP address, account login information and password, mobile advertising	Advertising, marketing, and analytics regarding our advertising and marketing efforts, including market research and surveys we conduct

ID, social security number, IP address, mobile ad ID, social media handles Protected Class Information: Gender, race and ethnicity information, age over 40 Commercial information: Records of products considered or purchased; other purchasing or consumer histories or tendencies Internet or other electronic activity information: your device and browser type, operating systems, device ID, your browsing and search history on our website and other sites; data captured by cookies and similar tracking technologies regarding your interaction with our websites and mobile apps Health data: data about your health condition or diagnosis or health data inferences Inferences drawn from personal information we collect	
Personal identifiers: name, email address, telephone numbers Professional information: job title, information about your employer Visual information: photographs taken for security purposes to enter our facilities	Business transactions and contracting with vendors and suppliers, including to audit or conduct diligence with the entity you represent
Personal identifiers: Full name, personal or professional postal and/or email address, phone number, governmental ID information, date of birth, pseudonymous identifiers Health data: data about your health condition or diagnosis or health data inferences	Conduct and recruit for our clinical trials, monitoring for drug safety and interactions
Personal identifiers: Full name, personal or professional postal and/or email address, phone number, governmental ID information, date of birth, IP address, account login information and password, mobile advertising ID, social security number, IP address, mobile ad ID, social media handles Protected Class Information: Gender, race and ethnicity information, age over 40 Commercial information: Records of products considered or purchased; other purchasing or consumer histories or tendencies Internet or other electronic activity information: your device and browser type, operating systems, device ID, your browsing	To monitor or improve our Sites and for internal business analysis

and search history on our website and other sites; data captured by cookies and similar tracking technologies regarding your interaction with our websites and mobile apps Health data: data about your health condition or diagnosis or health data inferences Inferences drawn from personal information we collect	
Personal identifiers: Full name, personal or professional postal and/or email address, phone number, governmental ID information, date of birth, IP address, account login information and password, mobile advertising ID, social security number, IP address, mobile ad ID Internet or other electronic activity information: your device and browser type, operating systems, device ID, your browsing and search history on our website and other sites; data captured by cookies and similar tracking technologies regarding your interaction with our websites and mobile apps	To prevent fraud and provide security services, activities that violate our Terms of Service or that are illegal; and to protect our rights and the rights and safety of our users or others

8. NOTICE AT COLLECTION: DE-IDENTIFICATION.

We may, in accordance with applicable US Privacy Law, de-identify your Personal Information, which means we take reasonable measures to remove or modify data so that it can no longer reasonably be linked to you or any other individual. We will continue to use and maintain the information in de-identified form and will not attempt to re-identify it, except as necessary to verify compliance with legal requirements. If we disclose de-identified data to third parties, we will require them to commit not to attempt re-identification. Once the information is de-identified, it is no longer considered Personal Information or subject to this Notice.

9. NOTICE AT COLLECTION: RETENTION PERIODS

When retaining and storing information about you in our systems, we have put in place data retention schedules in accordance with our company policy and in compliance with Applicable Data Protection Laws. When assessing the appropriate retention period, we take into account the quantity, nature and sensitivity of Personal Data, the potential risk of harm in the event of unauthorized use or disclosure, the purposes of the Processing and whether or not these purposes can be achieved by other means, as well as applicable legal obligations.

10. NOTICE AT COLLECTION: CATEGORIES OF PERSONAL INFORMATION WE SELL OR SHARE OR USE FOR TARGETED ADVERTISING

When we engage in digital advertising, we sell the following categories of personal information (according to the broad definition of “sell” under select state privacy laws), share them for purposes of cross-context behavioural advertising, or use them for targeted advertising: personal

identifiers (including IP address, mobile advertising IDs), internet or other electronic activity information, inferences.

These categories of personal information are sold to or shared for cross-context behavioural advertising or targeted advertising with advertising networks and other companies that facilitate or engage in digital advertising. We engage in such sales and sharing to provide you with marketing information and to help us understand which of our products or programs you are most likely to be interested in learning about. We do so by allowing third parties to place cookies or other tracking technologies on our website that may collect information about your online activities over time and across different websites or applications. For more information about the use of cookies and other tracking technologies, see the section "Cookies and Tracking Technologies" below.

To opt out of such sales and sharing of personal information, please call 855-961-0474 or complete the online form at: www.bms.com/dpo/us/request.

11. SOURCES FROM WHICH WE COLLECT PERSONAL INFORMATION

BMS collects information from you and the devices you use (including medical devices we may provide to you), health care providers and others who assist in the provision of or payment for your health care, data brokers and advertising partners. We may also collect information about you when you visit our facilities or offices.

12. USE OR DISCLOSURE OF SENSITIVE PERSONAL INFORMATION

BMS uses and discloses information that is defined as "sensitive personal information" or "sensitive data" under US Privacy Law.

We may use sensitive personal information to infer information about you that we use to market to you products in which you may be interested. California residents have the right to opt-out of the use of your sensitive personal information for that purpose and direct us to limit your use of such information for purposes such as providing requested products or services to you or for security purposes. You can exercise your right to limit by contacting BMS at 855-961-0474 or complete the online form at: www.bms.com/dpo/us/request.

We do not use sensitive personal information to create inferences about you that are used to make decisions about the provision or denial of health care or access to essential goods or services, or any other legally or similarly significant decisions.

13. PROFILING AND AUTOMATED DECISION-MAKING

We may use automated processing of personal information to create profiles about individuals. However, we do not use such profiles to make decisions that produce legal or other similarly significant effects, such as the provision or denial of financial or lending services, housing, insurance, education enrolment or opportunity, criminal justice, employment opportunities, health care services, or access to essential goods or services without meaningful human involvement unless someone will be involved to validate decisions resulting from such use.

14. DISCLOSURE OF PERSONAL INFORMATION FOR BUSINESS PURPOSES

As a multinational company operating worldwide, your personal information may be disclosed to, or accessed by, parties located outside your country of residence. If you are located outside of the United States, BMS may disclose your personal information to parties located in countries that provide less protection than in your country, which includes the United States.

Below you can find more information about the types of entities with to which BMS discloses and has disclosed your personal information for business purposes in the 12 months preceding the date of this Notice.

Disclosing your personal information within the BMS Group

We disclose your personal information within the BMS group of companies ("BMS Group") to facilitate the delivery of our products and services across different companies within the BMS Group, the operate the BMS Group companies, and for marketing purposes. This may include the Bristol Myers Squibb Company headquarters in the United States and all of its subsidiaries, branch offices, affiliates, entities and other companies that are part of, majority owned or controlled by, the BMS Group. When exchanging information internally, we rely on appropriate arrangements and mechanisms to cover any transfer of your personal information within our corporate structure, such as binding corporate rules (BCRs), contractual arrangements approved by authorities or based on consent, and data processing agreements.

Disclosing your personal information with processors/service providers/contractors

To conduct our business, we disclose personal information to entities that assist us in providing our products, services, and other business purposes. The categories of personal information we disclose to these entities for the purposes described below are personal identifiers, protected class information, financial and insurance information, commercial information, audio and visual information, internet and other electronic use information, geolocation, health data, and inferences we make from personal information:

- **Processors / service providers / contractors** that assist in providing information technology services, patient support services, call center and customer service-related services, order fulfilment, payment processing, shipping services, clinical trials and studies support, marketing or market research services, events, meeting and planning services, newsletters and other communications, services related to talent acquisition or consultancy, legal and accounting services, security and fraud detection, patient and drug safety and monitoring services

- **Business partners** such as external scientists and healthcare professionals to review and assist us with healthcare compliance activities and institutions and other organizations with whom we collaborate to support our clinical studies and patient support programs

Disclosing your personal information for legal or regulatory purposes

- **Regulatory and health authorities** including governmental bodies (such as the FDA, EMA, NHS), data protection authorities, tax authorities, or courts in case of disputes, when permitted or required by Applicable Data Protection Law

- **Entities to whom BMS reasonably believes it is legally obligated to provide such information or when disclosure is otherwise necessary to protect our rights and the rights and property, or the rights, property or safety of others**, such as other parties in litigation or legal disputes, guardians, conservators, or individuals with powers of attorney.

Data sharing in connection with a transfer of control

Circumstances may arise where we decide to reorganize or divest part or all of our business or a line of our business (or any portion of our assets), including our information databases and websites, through a sale, divestiture, merger, acquisition, in the event of a bankruptcy, or other means of transfer. In any such circumstance, your personal information may be shared with, sold, transferred, rented, licensed, or otherwise provided or made available by us or on our behalf to

actual or potential parties to, and in connection with, the contemplated transaction (without your consent or any further notice to you). In such circumstances, we will seek written assurances that personal information about you submitted through this Website will be protected appropriately.

15. OUR USE OF COOKIES AND ANALYTICS

We may use cookies, pixel tags, web beacons and other similar tracking technologies ("tracking technologies") to automatically collect information through our websites. Tracking technologies are small data files placed on your computer, tablet, mobile phone, or other devices that record certain pieces of information when you visit our website(s). We may use these tracking technologies to help identify irregular behavior, prevent fraudulent activity and improve security, as well as making it possible for you to save your preferences and help us understand how you interact with our Services.

We also allow third parties (including Google and Meta) to use third party cookies, web beacons, and other storage technologies to collect or receive information about how you interact with our websites and apps and elsewhere on the Internet and use that information to provide analytics and other measurements services, and to deliver and target advertisements tailored to you. Third parties may also use some of these technologies to assist us in determining if you require assistance or are having problems navigating on our websites or apps, and this may include technologies that record your interactions with the website or app, including without limitation, your keystrokes, mouse clicks, screen touches, and information about when, how and from where you accessed our website or app.

You may set your browser to notify you when you receive a cookie. Many web browsers also allow you to block cookies. You can disable cookies from your computer system by following the instructions on your browser or at www.youradchoices.com.

We use Google Analytics to evaluate the use of our website. Google Analytics uses cookies and other identifiers to collect information, such as how often users visit a Site, what pages they visit when they do so, and what other websites they visited prior to visiting our website. For information about Google's privacy practices, please refer to the Google Privacy Policy: https://policies.google.com/privacy?hl=en-US#infocollect. We also use Google reCAPTCHA, Google SEO, and Google APIs.

16. OPT-OUT PREFERENCE SIGNALS – DO NOT TRACK AND OTHERS

An opt-out preference signal is sent by a platform, technology, or mechanism on behalf of consumers and communicates a consumer's choice to opt out of the sale and sharing of personal information for cross-context behavioral advertising with all businesses that recognize the signal, without having to make individualized requests. The signal can be set on certain browsers or through opt-out plug-in tools.

We recognize the Global Privacy Control signal and do so at the browser level and it does not apply to personal information we may collect offline or that we may associate only with your name or email address. This means that if the signal is sent through a specific browser, we will recognize it for that browser only, and only with respect to the identifiers for that browser. If you would like more information about opt-out preference signals, including how to use them, the Global Privacy Control website has such information (https://globalprivacycontrol.org/).

We do not recognize the "do not track" or "DNT" signal that was developed in the early 2000s but not widely adopted.

17. PERSONAL INFORMATION OF MINORS

Our products and website are not directed to minors under the age of 13 and we do not knowingly sell or share for purposes of behavioural advertising the personal information of minors, including minors under 16 years of age

18. THIRD PARTY WEBSITES

Our website(s) may contain links to third-party websites, including social media buttons that link to social media platforms. This Notice does not govern how those third parties or social media platforms collect or use personal information, and we do not endorse or have control over their practices. The privacy policies and terms of use for those third parties' websites/apps or social media platforms govern those companies' privacy practices. We are not responsible for the content or privacy practices of any third-party websites or platforms.

19. HOW WE KEEP YOUR PERSONAL INFORMATION SECURE

We implement reasonable and appropriate technical and organizational controls to protect your personal information from unauthorized Processing, loss of data, disclosure, use, alteration, or destruction. However, there is no perfect security, and reasonable security is a process that involves risk management rather than risk elimination. While we are committed to maintaining a reasonable information security program, no such program can be perfect; in other words, all risk cannot reasonably be eliminated. Data security incidents and breaches can occur due to factors that cannot reasonably be prevented. Accordingly, it cannot be assumed that the occurrence of any given incident or breach results from our failure to implement and maintain reasonable security.

20. CHANGES TO THIS NOTICE

We will review and update this Notice from time to time. When we make material changes, we will prominently notify you by posting a clear notice on our website and updating the Privacy Policy accordingly. We encourage you to regularly visit this page to review the most current version of our Privacy Policy for the latest information on our privacy practices.

21. ACCESSIBILITY

To make accessibility-related requests or report barriers, please contact us using the information below.

22. CONTACT US

If you have questions about this Notice, to request a copy of it in another format, or for other questions, please contact our Data Protection Officer dpo@bms.com. You may also contact us at you may contact us Bristol-Myers Squibb Company, P.O. Box 640, Palatine, IL 60078-0640, 800-332-2056.

23. US STATE DATA PRIVACY RIGHTS

Consumer Rights Under US Privacy Laws

State privacy laws exist in California, Colorado, Connecticut, Delaware, Iowa, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Texas, and Utah, and Virginia give state residents various rights with respect to many types of personal information we collect about them, with some exceptions. Laws in Indiana (effective January 1, 2026); Kentucky (effective January 1, 2026), Maryland (effective October 1, 2025), Rhode Island (effective January 1, 2026) and Tennessee (July 1, 2025) are not in effect as of the date of this Privacy Policy; we will respond to requests made under such laws as of their effective date.

The rights provided under these laws are similar in many respects, with some differences from state to state. We list below the rights that may be applicable to our business under these laws:

Right to Know: The right to confirm whether or not we are processing a resident's personal information and to access such data. Laws in some states provide the right to know more detailed information.

- California's privacy law gives residents the right to request the following additional information collected since January 1, 2022: Categories of personal information we have collected about them; categories of sources from which such personal information was collected; categories of personal information that the business sold or disclosed for a business purpose about the consumer; categories of third parties to whom the personal information was sold or disclosed for a business purpose; and the business or commercial purpose for collecting or selling your personal information.

- Oregon's privacy law gives residents the right to request a list of third-party entities to which we have disclosed personal information.

Right to Access / Copy: The right to access or request a copy of the personal information we have collected from the resident, subject to certain exceptions.

Right to Delete: The right to request deletion of their personal information that we have collected from or about the resident and to have such information deleted, subject to certain exceptions.

Right to Correct: The right to request that we correct inaccuracies in the resident's personal information, taking into account the nature of personal data and purposes of processing such information.

Right to Limit the Use of Sensitive Personal Information: California's law gives residents the right to request that we not use or disclose their sensitive personal information for inferring characteristics about a consumer or for purposes other than to provide goods and services, protect and investigate fraud and other security-related issues, non-personalized advertising, and similar purposes described in the law.

Rights to Opt-Out: Rights to request that we stop using the resident's personal information for one or more of the following purposes:

- Sale of Personal Information: The right to request that we stop selling their personal information, consistent with the definition of "sale" in each law.

- Targeted Advertising: The right to request that we stop processing their personal information for targeted advertising, subject to exceptions in some state laws.

- Sharing for Cross-Context Behavioural Advertising: California's law provides the right to request that we stop sharing personal information for cross-context behavioural advertising.

Right to Revoke Consent: Depending on your place of residence and applicable US Privacy Law, you have the right to withdraw your consent for processing your Sensitive Information, effective for any future processing activities.

Please note, not all laws provide for all of these rights; we will respond to requests in accordance with your state's law. Additionally, California's law is the only law that applies to all state residents, irrespective of the context in which they interact with us (e.g., a customer, a business contact, a vendor). Laws in other states apply only to people when acting in an individual or household context.

Consumer Rights Under U.S. State Consumer Health Data Privacy Laws

We have a separate Consumer Health Data Privacy Notice that relates to rights provided under consumer health data privacy laws in Nevada and Washington state to residents of those states acting in an individual or household context with respect to their consumer health data. Washington's law may also apply to individuals whose consumer health data is processed in that state. Access to our Consumer Health Data Privacy Notices are provided here: **Washington Consumer Health Data Privacy Notice** and **Nevada Consumer Health Data Privacy Notice**.

California Shine the Light

With reference to California Civil Code Section 1798.83, also known as the "Shine the Light" law, we allow California residents to opt out of the disclosure of personal information to third parties for third parties' direct marketing purposes. To exercise that opt-out option, by contacting BMS at 855-961-0474 or complete the online form at: www.bms.com/dpo/us/request.

Exercising Your Rights

We will respond to requests from residents of states with data privacy laws that apply to us and will do so with respect to the rights that are provided under the requestor's state law as of the effective date of that law. The laws in some states listed above may not be in effect as of the date of this Privacy Policy.

To exercise rights to know, access/copy, delete, correct, or know third parties to whom personal information is disclosed, please contact BMS at 855-961-0474 or complete the online form at: www.bms.com/dpo/us/request. We will provide a substantive response to these requests within 45 days of the date on which we receive your request. If we require additional information or time to process your requests, we will contact you.

To exercise the right to limit the use of sensitive personal information, please contact BMS at 855-961-0474 or complete the online form at: www.bms.com/dpo/us/request.

To exercise opt-out rights, submit your request here.

Exercising Your Rights Using Authorized Agents

Agents may submit opt-out requests on behalf of individuals under several state data privacy laws; this is not an option that is available under laws in Texas, Utah, or Virginia. California residents can also designate an agent to submit all other types of data subject requests. If the agent submits an opt-out request on your behalf, the agent will need to provide us with your signed permission indicating the agent has been authorized to submit the opt-out request on your behalf. Agents can submit opt-out requests here.

If you are a California resident and you use an agent to submit requests to know, access/copy, delete, or correct, the agent will need to provide us with your signed permission indicating the agent has been authorized to submit the request on your behalf. You will also be required to verify your identity directly with us or confirm with us that you provided the agent with permission to submit the request. Agents can submit requests on behalf of California residents (other than opt-out requests) please contact BMS at 855-961-0474 or complete the online form at: www.bms.com/dpo/us/request.

Please note that this subsection does not apply when an agent is authorized to act on your behalf pursuant to a valid power of attorney. Any such requests will be processed in accordance with state law pertaining to powers of attorney.

Verification of Requests
When you exercise rights other than opt-out rights and the right to limit collection of sensitive personal information, we will take steps to verify your identity. We will ask you for at least two pieces of personal information, depending on the nature of the request, and attempt to match those to information that we maintain or collect about you.

If we are unable to verify your identity with the degree of certainty required, we will not be able to respond to the request. We will notify you to explain the basis of the denial.

When We Do Not Act on a Request – Appeal Process

In some cases, we may not act on your requests (e.g., if we cannot do so under other laws that apply). When this is the case, we will explain our reasons for not providing you with the information or taking the action (e.g., correcting data) you requested.

Additionally, you may have the right to appeal our decision by contacting us at same method used to submit requests within 30 days after your receipt of our decision.

24. JOB APPLICANT NOTICE

BMS may Process your personal information to evaluate your application to work at BMS ("Applicant Personal Information"). Below, you can find more information about how BMS Processes Applicant Personal Information when you apply to work for us.

Notice at Collection: Categories of Applicant Personal Information We Collect

- **Professional and Education Information:** Job title, education information, professional qualifications, work experience, publications, and professional networks, programs and activities in which you participated
- **Personal Identifiers:** e-mail address, full name, address, phone numbers, date of birth and other contact information you may provide, application portal log in information
- **Internet and other electronic activity information:** your device and browser type, operating systems, device ID, your browsing and search history on our website and other sites
- **Protected class information:** Race, ethnicity, gender, gender identification, veteran status[1]

We have collected the same categories of Applicant Personal Information in the 12 months prior to the date of this Privacy Notice.

Notice at Collection: Purposes for Collection of Applicant Personal Information

We use Applicant Personal Information to evaluate your application for employment, to conduct job interviews, and to comply with applicable law.

Notice at Collection: Categories of Personal Information We Sell or Share

We do not sell or share for cross-context behavioural advertising Applicant Personal Information.

Notice at Collection: Retention Periods

We retain the categories of Applicant Personal Information for the length of time necessary to evaluate applicants, comply with legal obligations and to protect our legal rights.

Sources From Which We Collect Personal Information

We collect Applicant Personal Information from applicants directly, from recruiters, from any references or professional contacts that may provide references or other information about applicants, from our employees or contractors that may interview or otherwise evaluate applicants, and from publicly available sources.

Use or Disclosure of Sensitive Personal Information

We do not use or disclose sensitive Applicant Personal Information to infer characteristics about applicants or for any purposes other than to identify applicants to comply with applicable laws or to operate our business, including by evaluating applicants.

Disclosure of Personal Information for Business Purposes in the Past 12 Months

The following chart describes the categories of Applicant Personal Information that we disclosed to third parties for a business purpose in the 12 months prior to the date of this Notice:

Categories of Applicant Personal Information	**Purposes for Disclosure of Applicant Personal Information to Service Providers or Contractors**
Personal identifiers: name, address, email address	Human resource functions; scheduling and email communications; security services and cloud-based data storage, IT-related functions; legal services
Internet or other electronic network activity information	Security services and cloud-based data storage, website hosting, other IT-related functions
Professional information: records of your work and education history	Recruitment support
Educational information: Education history; trade school records; certificates obtained	Recruitment support

Additional Information About How We May Disclose Applicant Personal Information

We may also share Applicant Personal Information as required or permitted by law to comply with a subpoena or similar legal process or government request, or when we believe in good faith that disclosure is legally required or otherwise necessary to protect our rights and property or the rights, property or safety of others, including to law enforcement agencies, and judicial and regulatory authorities. We may also share Applicant Personal Information with third parties to help detect and protect against fraud or data security vulnerabilities. And we may share or transfer Applicant Personal Information to a third party in the event of an actual or potential sale, merger, reorganization of our entity or other restructuring.

Rights Related to Applicant Personal Information

Job applicants have the following rights with respect to Applicant Personal Information, subject to exceptions in California law. To submit requests, please contact BMS at 855-961-0474 or complete the online form at: www.bms.com/dpo/us/request.

- **Access and Disclosure** – The right to know the categories of Applicant Personal Information we have collected, purposes for collection, sources, categories of Applicant Personal information we sold or disclosed for a business purpose, and the categories of recipients of such disclosures. You also have a right to a copy of your Applicant Personal Information. This relates to Applicant Personal Information we have collected since January 1, 2022.

- **Deletion** - The right to request that we delete your Applicant Personal Information.

- **Correction** – The right to request that we correct your Applicant Personal Information.

If you are a California resident and you use an agent to submit requests to know, access/copy, delete, or correct, the agent will need to provide us with your signed permission indicating the agent has been authorized to submit the request on your behalf. You will also be required to verify your identity directly with us or confirm with us that you provided the agent with permission to submit the request. Agents can submit requests on behalf of California residents please contact BMS at 855-961-0474 or complete the online form at: www.bms.com/dpo/us/request.

Please note that this subsection does not apply when an agent is authorized to act on your behalf pursuant to a valid power of attorney. Any such requests will be processed in accordance with state law pertaining to powers of attorney.